

# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/015085

International filing date: 18 August 2005 (18.08.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP  
Number: 2004-239465  
Filing date: 19 August 2004 (19.08.2004)

Date of receipt at the International Bureau: 13 October 2005 (13.10.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2004年 8月19日

出 願 番 号  
Application Number: 特願2004-239465

パリ条約による外国への出願  
に用いる優先権の主張の基礎  
となる出願の国コードと出願  
番号  
The country code and number  
of your priority application,  
to be used for filing abroad  
under the Paris Convention, is

J P 2004-239465

出 願 人  
Applicant(s): 日本電信電話株式会社

2005年 9月28日

特許庁長官  
Commissioner,  
Japan Patent Office

中 嶋



【書類名】 特許願  
【整理番号】 NTTH165228  
【提出日】 平成16年 8月19日  
【あて先】 特許庁長官殿  
【国際特許分類】 G09C 1/00  
【発明者】  
    【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内  
    【氏名】 堀田 英一  
【発明者】  
    【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内  
    【氏名】 小野 諭  
【発明者】  
    【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内  
    【氏名】 石本 英隆  
【発明者】  
    【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内  
    【氏名】 田倉 昭  
【特許出願人】  
    【識別番号】 000004226  
    【氏名又は名称】 日本電信電話株式会社  
【代理人】  
    【識別番号】 100083806  
    【弁理士】  
    【氏名又は名称】 三好 秀和  
    【電話番号】 03-3504-3075  
【手数料の表示】  
    【予納台帳番号】 001982  
    【納付金額】 16,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1  
    【包括委任状番号】 9701396

## 【書類名】特許請求の範囲

### 【請求項1】

所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの前記要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記証明装置のイベント順序証明方法であって、

前記利用者装置からの前記要求を受信する順序証明要求受信ステップと、

前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算ステップと、

前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を接続した接続値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約ステップと、

前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む証明書を作成する証明書作成ステップと、

前記証明書を前記利用者装置に送信する証明書送信ステップと、

前記利用者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、

前記利用者装置からの前記要求を前記順次集約木に割り当てた以後に、監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、監査用証明書を作成するとともに、前記監査用の前記要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、該監査用証明書に含める監査用証明書作成ステップと、

前記監査用証明書を前記監査装置に送信する監査用証明書送信ステップと、

前記監査用の要求を前記順次集約木に割り当てた以後に、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信ステップと、

前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成ステップと、

前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信ステップと、  
を有することを特徴とするイベント順序証明方法。

### 【請求項2】

前記証明書は、前記証明書の即時補完情報を含むことを特徴とする請求項1記載のイベント順序証明方法。

### 【請求項3】

前記監査用証明書作成ステップは、さらに、前記利用者装置からの前記要求を前記順次集約木に割り当てた以前に、監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、監査用証明書を作成するとともに、前記監査用の前記要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、該監査用証明書に含めるステップを備え、

前記一定時間間隔終了後に前記監査用証明書作成ステップで作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成ステップと、

前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信

ステップと、

を有することを特徴とする請求項 1 又は 2 記載のイベント順序証明方法。

【請求項 4】

前記順次割当データは、前記要求に含まれるデジタル情報に対して所定の衝突困難一方向関数を適用した結果値であることを特徴とする請求項 1 乃至 3 のいずれか 1 項に記載のイベント順序証明方法。

【請求項 5】

前記証明書は、デジタル署名が施されていることを特徴とする請求項 1 乃至 4 のいずれか 1 項に記載のイベント順序証明方法。

【請求項 6】

前記一定時間間隔終了後に前記順次集約木のルート値を電子的に公表する電子的情報公表ステップを有することを特徴とする請求項 1 乃至 5 のいずれか 1 項に記載のイベント順序証明方法。

【請求項 7】

前記証明装置は、複数の前記要求を前記順次集約木に順次割り当てたときは、割り当てた時間的順序で、前記複数の要求に対する証明書を送信する手段を有することを特徴とする請求項 1 乃至 6 のいずれか 1 項に記載のイベント順序証明方法。

【請求項 8】

所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの該要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記監査装置のイベント順序証明監査方法であって

前記証明装置は、

前記利用者装置からの前記要求を受信する順序証明要求受信手段と、

前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、

前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに 1 つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を接続した接続値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、

前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第 1 の順次集約木特定情報を含む証明書を作成する証明書作成手段と、

前記証明書を前記利用者装置に送信する証明書送信手段と、

前記利用者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、

複数の監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、前記複数の監査用の前記要求を前記順次集約木に割り当てた時点におけるそれぞれの監査用の前記即時補完情報を前記順次集約木から取得し、前記複数の監査用証明書に含める監査用証明書作成手段と、

前記監査用証明書を前記監査装置に送信する監査用証明書送信手段と、

前記証明書送信後、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、

前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第 2 の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取

得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、

前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、  
を有し、

前記証明装置から、前記複数の監査用証明書を受信する監査用証明書受信ステップと、  
前記利用者装置から、前記証明書及び前記遅延補完情報を含む前記証明書に対する監査要求を受信する監査要求受信ステップと、

受信した複数の監査用証明書の中から、受信した監査要求の第1及び第2の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より生成された時間的順序が後、かつ遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第1の監査用証明書選択ステップと、

前記順次集約木の特定のノードに対して、前記第1の監査用証明書選択ステップで選択された監査用証明書に含まれる該ノードの割当値と、前記監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第1の証明書監査ステップと、

前記証明書の監査結果を前記利用者装置に送信する監査結果送信ステップと、  
を有することを特徴とするイベント順序証明監査方法。

#### 【請求項9】

前記監査用証明書受信ステップは、前記監査用証明書を受信する第1の時刻を時刻提供装置から取得するステップを有し、

前記第1の証明書監査ステップは、前記証明書の要求受付が前記第1の時刻よりも時間的に前であることを示す区間時刻証を監査結果に含めることを特徴とする請求項8記載のイベント順序証明監査方法。

#### 【請求項10】

前記証明装置は、  
前記一定時間間隔終了後に前記監査用証明書作成手段で作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成手段と、

前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、  
を有し、

受信した複数の監査用証明書の中から、受信した監査要求の第1の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より時間的順序が前の監査用証明書を選択する第2の監査用証明書選択ステップと、

前記順次集約木の特定のノードに対して、前記監査要求に含まれる該ノードの割当値と、前記第2の監査用証明書選択ステップで選択された監査用証明書及び該監査用証明書の遅延補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第2の証明書監査ステップと、

を有することを特徴とする請求項8又は9記載のイベント順序証明監査方法。

#### 【請求項11】

複数の証明書に対する各監査結果と、前記複数の証明書の第1の順次集約木特定情報に基づいて、前記複数の証明書間における要求受付の時間的順序を判定する利用者間順序判定ステップと、を有し、

前記監査結果送信ステップは、前記複数の証明書間における要求受付の時間的順序を前記監査結果に含めることを特徴とする請求項10記載のイベント順序証明監査方法。

#### 【請求項12】

前記監査用証明書及び該監査用証明書の遅延補完情報から前記順次集約木のルート値を計算するルート値計算ステップと、

電子的に公表された前記順次集約木のルート値と計算されたルート値が一致するか否かの検証を行うルート値検証ステップと、

を有することを特徴とする請求項10又は11記載のイベント順序証明監査方法。

【請求項13】

前記第1の監査用証明書選択ステップで選択された監査用証明書及び該監査用証明書の遅延補完情報を前記利用者装置に送信する監査用補完情報送信ステップを有することを特徴とする請求項10乃至12のいずれか1項に記載のイベント順序証明監査方法。

【請求項14】

前記監査用証明書受信ステップは、監査用の前記要求を前記証明装置に送信する第2の時刻を時刻提供装置から取得するステップを有し、

前記第2の証明書監査ステップは、前記証明書の要求受付が前記第2の時刻より時間的に後であることを示す区間時刻証を監査結果に含めることを特徴とする請求項10乃至13のいずれか1項に記載のイベント順序証明監査方法。

【請求項15】

前記監査結果は、デジタル署名が施されていることを特徴とする請求項8乃至14のいずれか1項に記載のイベント順序証明監査方法。

【請求項16】

所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの前記要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記証明装置であって、

前記利用者装置からの前記要求を受信する順序証明要求受信手段と、

前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、

前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を接続した接続値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、

前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む証明書を作成する証明書作成手段と、

前記証明書を前記利用者装置に送信する証明書送信手段と、

前記利用者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、

前記利用者装置からの前記要求を前記順次集約木に割り当てた以後に、監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、監査用証明書を作成するとともに、前記監査用の前記要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、該監査用証明書に含める監査用証明書作成手段と、

前記監査用証明書を前記監査装置に送信する監査用証明書送信手段と、

前記監査用の要求を前記順次集約木に割り当てた以後に、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、

前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、

前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、  
を有することを特徴とする証明装置。

【請求項 17】

前記証明書は、前記証明書の即時補完情報を含むことを特徴とする請求項 16 記載の証明装置。

【請求項 18】

前記監査用証明書作成手段は、さらに、前記利用者装置からの前記要求を前記順次集約木に割り当てた以前に、監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、監査用証明書を作成するとともに、前記監査用の前記要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、該監査用証明書に含める手段を備え、

前記一定時間間隔終了後に前記監査用証明書作成手段で作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成手段と、

前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、  
を有することを特徴とする請求項 16 又は 17 記載の証明装置。

【請求項 19】

前記順次割当データは、前記要求に含まれるデジタル情報に対して所定の衝突困難一方向関数を適用した結果値であることを特徴とする請求項 16 乃至 18 のいずれか 1 項に記載の証明装置。

【請求項 20】

前記証明書は、デジタル署名が施されていることを特徴とする請求項 16 乃至 19 のいずれか 1 項に記載の証明装置。

【請求項 21】

前記一定時間間隔終了後に前記順次集約木のルート値を電子的に公表する電子的情報公表手段を有することを特徴とする請求項 16 乃至 20 のいずれか 1 項に記載の証明装置。

【請求項 22】

前記証明装置は、複数の前記要求を前記順次集約木に順次割り当てたときは、割り当てた時間的順序で、前記複数の要求に対する証明書を送信する手段を有することを特徴とする請求項 16 乃至 21 のいずれか 1 項に記載の証明装置。

【請求項 23】

所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの該要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記監査装置であって、

前記証明装置は、

前記利用者装置からの前記要求を受信する順序証明要求受信手段と、

前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、

前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに 1 つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を接続した接続値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、

前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第 1 の順次集約木特定情報を含む証明書を作成する証明書作成手段と、

前記証明書を前記利用者装置に送信する証明書送信手段と、



前記利用者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、

複数の監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、前記複数の監査用の前記要求を前記順次集約木に割り当てた時点におけるそれぞれの監査用の前記即時補完情報を前記順次集約木から取得し、前記複数の監査用証明書に含める監査用証明書作成手段と、

前記監査用証明書を前記監査装置に送信する監査用証明書送信手段と、

前記証明書送信後、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、

前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、

前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、  
を有し、

前記証明装置から、前記複数の監査用証明書を受信する監査用証明書受信手段と、

前記利用者装置から、前記証明書及び前記遅延補完情報を含む前記証明書に対する監査要求を受信する監査要求受信手段と、

受信した複数の監査用証明書の中から、受信した監査要求の第1及び第2の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より生成された時間的順序が後、かつ遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第1の監査用証明書選択手段と、

前記順次集約木の特定のノードに対して、前記第1の監査用証明書選択手段で選択された監査用証明書に含まれる該ノードの割当値と、前記監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第1の証明書監査手段と、

前記証明書の監査結果を前記利用者装置に送信する監査結果送信手段と、  
を有することを特徴とする監査装置。

#### 【請求項24】

前記監査用証明書受信手段は、前記監査用証明書を受信する第1の時刻を時刻提供装置から取得する手段を有し、

前記第1の証明書監査手段は、前記証明書の要求受付が前記第1の時刻よりも時間的に前であることを示す区間時刻証を監査結果に含めることを特徴とする請求項23記載の監査装置。

#### 【請求項25】

前記証明装置は、

前記一定時間間隔終了後に前記監査用証明書作成手段で作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成手段と、

前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、  
を有し、

受信した複数の監査用証明書の中から、受信した監査要求の第1の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より時間的順序が前の監査用証明書を選択する第2の監査用証明書選択手段と、

前記順次集約木の特定のノードに対して、前記監査要求に含まれる該ノードの割当値と、前記第2の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延

補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第2の証明書監査手段と、  
を有することを特徴とする請求項23又は24記載の監査装置。

【請求項26】

複数の証明書に対する各監査結果と、前記複数の証明書の第1の順次集約木特定情報に基づいて、前記複数の証明書間における要求受付の時間的順序を判定する利用者間順序判定手段と、を有し、

前記監査結果送信手段は、前記複数の証明書間における要求受付の時間的順序を前記監査結果に含めることを特徴とする請求項25記載の監査装置。

【請求項27】

前記監査用証明書及び該監査用証明書の遅延補完情報から前記順次集約木のルート値を計算するルート値計算手段と、

電子的に公表された前記順次集約木のルート値と計算されたルート値が一致するか否かの検証を行うルート値検証手段と、

を有することを特徴とする請求項25又は26記載の監査装置。

【請求項28】

前記第1の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延補完情報を前記利用者装置に送信する監査用補完情報送信手段を有することを特徴とする請求項25乃至27のいずれか1項に記載の監査装置。

【請求項29】

前記監査用証明書受信手段は、監査用の前記要求を前記証明装置に送信する第2の時刻を時刻提供装置から取得する手段を有し、

前記第2の証明書監査手段は、前記証明書の要求受付が前記第2の時刻より時間的に後であることを示す区間時刻証を監査結果に含めることを特徴とする請求項25乃至28のいずれか1項に記載の監査装置。

【請求項30】

前記監査結果は、デジタル署名が施されていることを特徴とする請求項25乃至29のいずれか1項に記載の監査装置。

【請求項31】

請求項1乃至7のいずれか1項に記載のイベント順序証明方法の各ステップを前記証明装置に実行させることを特徴とするイベント順序証明プログラム。

【請求項32】

請求項8乃至15のいずれか1項に記載のイベント順序証明監査方法の各ステップを前記証明監査装置に実行させることを特徴とするイベント順序証明監査プログラム。

【請求項33】

所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの前記要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記利用者装置のためのイベント順序証明検証プログラムであって、

前記証明装置は、

前記利用者装置からの前記要求を受信する順序証明要求受信手段と、

前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、

前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を接続した接続値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する

順序証明要求集約手段と、

前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む証明書を作成する証明書作成手段と、

前記証明書を前記利用者装置に送信する証明書送信手段と、

前記利用者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、

複数の監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、前記複数の監査用の前記要求を前記順次集約木に割り当てた時点におけるそれぞれの監査用の前記即時補完情報を前記順次集約木から取得し、前記複数の監査用証明書に含める監査用証明書作成手段と、

前記監査用証明書を前記監査装置に送信する監査用証明書送信手段と、

前記証明書送信後、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、

前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、

前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、  
を有し、

前記監査装置は、

前記証明装置から、前記複数の監査用証明書を受信する監査用証明書受信手段と、

前記利用者装置から、前記証明書及び前記遅延補完情報を含む前記証明書に対する監査要求を受信する監査要求受信手段と、

受信した複数の監査用証明書の中から、受信した監査要求の第1及び第2の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より生成された時間的順序が後、かつ遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第1の監査用証明書選択手段と、

前記順次集約木の特定のノードに対して、前記第1の監査用証明書選択手段で選択された監査用証明書に含まれる該ノードの割当値と、前記監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第1の証明書監査手段と、

前記証明書の監査結果を前記利用者装置に送信する監査結果送信手段と、  
を有し、

前記要求を前記証明装置に送信する順序証明要求送信ステップと、

前記証明装置から、前記証明書を受信する証明書受信ステップと、

前記証明書の補完情報の要求を前記証明装置に送信する補完情報要求送信ステップと、

前記証明装置から、前記補完情報を受信する補完情報受信ステップと、

前記監査要求を前記監査装置に送信する監査要求送信ステップと、

前記監査結果を受信する監査結果受信ステップと、

を前記利用者装置に実行させることを特徴とするイベント順序証明検証プログラム。

#### 【請求項34】

前記監査装置の前記監査用証明書受信手段は、前記監査用証明書を受信する第1の時刻を時刻提供装置から取得する手段を有し、

前記第1の証明書監査手段は、前記証明書の要求受付が前記第1の時刻よりも時間的に前であることを示す区間時刻証を監査結果に含め、

前記要求を前記証明装置に送信する時点の第3の時刻を前記時刻提供装置から取得し、

該第 3 の時刻を所定の手順に従って計算した値を前記要求に含める順序証明要求作成ステップを

前記利用者装置に実行させることを特徴とする請求項 3 3 記載のイベント順序証明検証プログラム。

【請求項 3 5】

前記証明装置は、

前記一定時間間隔終了後に前記監査用証明書作成手段で作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成手段と、

前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、

を有し、

前記監査装置は、

受信した複数の監査用証明書の中から、受信した監査要求の第 1 の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より時間的順序が前の監査用証明書を選択する第 2 の監査用証明書選択手段と、

前記順次集約木の特定のノードに対して、前記監査要求に含まれる該ノードの割当値と、前記第 2 の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第 2 の証明書監査手段と、

を有することを特徴とする請求項 3 3 又は 3 4 記載のイベント順序証明検証プログラム。

【請求項 3 6】

前記監査装置は、

複数の証明書に対する各監査結果と、前記複数の証明書の第 1 の順次集約木特定情報に基づいて、前記複数の証明書間における要求受付の時間的順序を判定する利用者間順序判定手段を有し、

前記監査結果送信手段は、前記複数の証明書間における要求受付の時間的順序を前記監査結果に含め、

前記監査要求は、他の証明書との時間的順序の判定要求を含むことを特徴とする請求項 3 5 記載のイベント順序証明検証プログラム。

【請求項 3 7】

前記監査装置は、

前記第 1 の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延補完情報を前記利用者装置に送信する監査用補完情報送信手段を有し、

前記監査装置から送信された監査用証明書及び該監査用証明書の遅延補完情報を受信するステップを前記利用者装置に実行させることを特徴とする請求項 3 5 記載のイベント順序証明検証プログラム。

【請求項 3 8】

前記監査用証明書受信手段は、監査用の前記要求を前記証明装置に送信する第 2 の時刻を時刻提供装置から取得する手段を有し、

第 2 の証明書監査手段は、前記証明書の要求受付が前記第 2 の時刻より時間的に後であることを示す区間時刻証を監査結果に含め、

前記要求を前記証明装置に送信する時点の第 3 の時刻を前記時刻提供装置から取得し、該第 3 の時刻を所定の手順に従って計算した値を前記要求に含める順序証明要求作成ステップを

前記利用者装置に実行させることを特徴とする請求項 3 4 乃至 3 7 のいずれか 1 項に記載のイベント順序証明検証プログラム。

【請求項 3 9】

前記証明装置から受信した証明書、及び前記一定時間間隔終了後に取得した該証明書の

補完情報すべてから、前記順次集約木のルート値を計算するルート値計算ステップと、

前記一定時間間隔終了後に電子的に公表された前記順次集約木のルート値と計算されたルート値が一致するか否かの検証を行うルート値検証ステップと、

を前記利用者装置に実行させることを特徴とする請求項 33 乃至 38 のいずれか 1 項に記載のイベント順序証明検証プログラム。

【請求項 40】

請求項 34 又は 38 記載のイベント順序証明検証プログラムを実行する利用者装置が前記要求に付した時刻を検証するコンピュータが読み取り可能なイベント時刻検証プログラムであって、

前記監査結果を取得する監査結果取得ステップと、

前記監査結果に対応する前記要求を取得する順序証明要求取得ステップと、

前記第 3 の時刻と、前記第 1 又は第 2 の時刻のうち少なくとも 1 以上との時間差に基づいて、前記第 3 の時刻の正当性を判定する時刻検証ステップと、

前記判定結果を出力するステップと、

前記コンピュータに実行させることを特徴とするイベント時刻検証プログラム。

【書類名】明細書

【発明の名称】 イベント順序証明方法及びイベント順序証明監査方法、イベント順序証明システムにおける証明装置及び監査装置、並びにイベント順序証明プログラム、イベント順序証明監査プログラム、イベント順序証明検証プログラム及びイベント時刻検証プログラム

【技術分野】

【0001】

本発明は、デジタル・データの生成を伴うイベントの生起順序を証明するイベント順序証明技術に関する。

【背景技術】

【0002】

イベント順序証明技術は、デジタル・データの生成を伴う複数のイベントの間の生起順序を証明するとともに、そのようなイベントに伴って生成されたデジタル・データが何であったかを証明する技術である。

【0003】

近年、インターネット上での電子商取引の活発化や、デジタル文書管理の利用拡大に伴い、「誰が、いつ、どんなデータを生成し、送信したか」を第三者が証明する電子公証の仕組みが必要とされている。電子公証は、送受信者の特定、到達確認、送受信等の前後関係の証明、改ざんの検知、電子文書保管等の機能を具備するものであるが、イベント順序証明技術は、このうち、前後関係の証明及び改ざんの検知の機能を実現するものである。

【0004】

図32は、このようなイベント順序証明技術を用いたイベント順序証明システムを説明する図である。同図に示すイベント順序証明システム900は、利用者（要求者、検証者）80がイベント順序証明の対象データをイベント順序証明装置90に送信すると、イベント順序証明装置90が利用者80から要求された対象データに対して受付の順番を示すデータを付したイベント順序受理証明書を生成し、該イベント順序受理証明書を利用者80に返信するようになっている。そして、イベント順序証明装置90で発行されたイベント順序受理証明書は、PKI（Public Key Infrastructure；公開鍵基盤）のもとでデジタル署名を主要な偽造防止／証明手段として採用する場合には、一般に、利用者80から送られた対象データに受付の順番を付した署名対象データに対するデジタル署名を含んだイベント順序受理証明書となっている。

【0005】

このイベント順序受理証明書の真正性の主要な根拠としてデジタル署名を用いるイベント順序証明システムに関しては、イベント順序証明装置90の不正、イベント順序受理証明書の有効期間、およびシステム運用の面などにおいて問題点が指摘されている。そのため、イベント順序受理証明書の真正性の主要な根拠としてデジタル署名を用いないイベント順序証明の方法も提案されている。例えば、線形リンク（Linear Linking Protocol）による方法（例えば、非特許文献1参照。）は、イベント順序証明装置90が仮に信頼できないとしてもシステム全体として高い安全性を確保することが可能となっている方法である。図33は、PKIに依存しない線形リンクによるイベント順序証明システムを説明する図である。同図に示すイベント順序証明システム910は、複数の利用者80のイベント順序証明対象データ（ハッシュ値）を相互に関連付けるリンク情報 $L_0$ を生成し、リンク情報 $L_0$ を含むイベント順序受理証明書を返信するようになり、各イベント順序受理証明書が、それまでに生成されたすべてのイベント順序受理証明書に依存するようになっている。そして、このリンク情報の一部（ $L_M$ 、 $L_N$ ）が定期的にマスメディア等（例えば新聞）に公表されるので、これにより、イベント順序証明装置90の不正を防止し、結果としてシステム全体の信頼を高めることができるようになっている。

【0006】

この線形リンクの方式については、イベント順序証明装置90の不正を検出するために利用者80相互の協力が必要であるという問題点、及び、利用者80が取得したイベント順

序受理証明書を検証、即ち、該イベント順序受理証明書と公表された情報が所定の方式で関係づけられることを検証するには利用者80はイベント順序証明装置90から大量のデータを取得する必要があるという問題点が指摘されている。

#### 【0007】

これらの問題の一部を解決するための方法も提案されている。例えば、非特許文献2においては、一定期間にイベント順序証明装置で処理されたイベント順序証明要求をまとめて公表するデータを計算するために、非特許文献1で使われている線形のリストの代わりに、木構造を用いることにより、利用者80がイベント順序受理証明書の検証を行うために必要なデータの量を、該一定期間に受け付けられるイベント順序証明要求の数に比例する量から、その対数(底2)に比例する量に著しく削減する方法を提案している。

【非特許文献1】S. Haber and W. Stornetta, How to Time-Stamp a Digital Document, Journal of Cryptology, Vol. 3, No. 2, pp. 99—111, 1991

【非特許文献2】A. Buldas, H. Lipmaa and B. Schoenmakers,

Optimally efficient accountable time-stamping, in Proceedings of Public Key Cryptography 2000 (PKC2000), eds. Y. Zheng and H. Imai, pp.293—305, Springer-Verlag, January 2000

#### 【発明の開示】

#### 【発明が解決しようとする課題】

#### 【0008】

しかしながら、上述した従来技術の木構造を用いる方式については、次のような問題点がある。

#### 【0009】

ある一定期間に異なる2つの利用者が各々イベント順序証明要求をイベント順序証明装置に送付し、それら要求が受理されたときにおいて、第1の利用者のある順序証明要求の受け付けが第2の利用者のある順序証明要求の受け付けより前になされたことの証明が、当該の期間が終了してイベント順序証明要求をまとめた公表データが公開されるまではできないという問題がある。即ち、当該の2つの順序証明要求と公表データが所定の方式で関係付けられることの検証が、公表データが公開されるまでできないという問題がある。このため、イベント順序証明システムに対する利用者の利便性が劣るとともに、イベント順序証明装置に障害が発生した時には、イベント順序受理証明書の検証ができないという欠点がある。

#### 【0010】

本発明は、上記の問題を解決するためになされたものであり、木構造を用いてイベント順序を証明するイベント順序証明システムにおいて、イベント順序証明要求をまとめた公表データを用いなくても、イベント順序証明機関から発行されたイベント順序受理証明書の検証を行うことができるイベント順序証明方法及びイベント順序証明監査方法、イベント順序証明システムにおける証明装置及び監査装置、並びにイベント順序証明プログラム、イベント順序証明監査プログラム、イベント順序証明検証プログラム及びイベント時刻検証プログラムを提供することを目的とする。

#### 【課題を解決するための手段】

#### 【0011】

上記目的を達成するため、請求項1記載の本発明は、所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの前記要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記証明装置のイベント順序証明方法であって、前記利用者装置からの前記要求を受信する順序証明要求受信ステップと、前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算ステップと、前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの

割当値を接続した接続値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約ステップと、前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む証明書を作成する証明書作成ステップと、前記証明書を前記利用者装置に送信する証明書送信ステップと、前記利用者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、前記利用者装置からの前記要求を前記順次集約木に割り当てた以後に、監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、監査用証明書を作成するとともに、前記監査用の前記要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、該監査用証明書に含める監査用証明書作成ステップと、前記監査用証明書を前記監査装置に送信する監査用証明書送信ステップと、前記監査用の要求を前記順次集約木に割り当てた以後に、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信ステップと、前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成ステップと、前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信ステップと、を有することを特徴とする。

【0012】

請求項2記載の本発明は、請求項1記載の発明において、前記証明書は、前記証明書の即時補完情報を含むことを特徴とする。

【0013】

請求項3記載の本発明は、請求項1又は2記載の発明において、前記監査用証明書作成ステップは、さらに、前記利用者装置からの前記要求を前記順次集約木に割り当てた以前に、監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、監査用証明書を作成するとともに、前記監査用の前記要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、該監査用証明書に含めるステップを備え、前記一定時間間隔終了後に前記監査用証明書作成ステップで作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成ステップと、前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信ステップと、を有することを特徴とする。

【0014】

請求項4記載の本発明は、請求項1乃至3のいずれか1項に記載の発明において、前記順次割当データは、前記要求に含まれるデジタル情報に対して所定の衝突困難一方向関数を適用した結果値であることを特徴とする。

【0015】

請求項5記載の本発明は、請求項1乃至4のいずれか1項に記載の発明において、前記証明書は、デジタル署名が施されていることを特徴とする。

【0016】

請求項6記載の本発明は、請求項1乃至5のいずれか1項に記載の発明において、前記一定時間間隔終了後に前記順次集約木のルート値を電子的に公表する電子的情報公表ステップを有することを特徴とする。

【0017】

請求項7記載の本発明は、請求項1乃至6のいずれか1項に記載の発明において、前記証明装置は、複数の前記要求を前記順次集約木に順次割り当てたときは、割り当てた時間的順序で、前記複数の要求に対する証明書を送信する手段を有することを特徴とする。



#### 【0018】

請求項8記載の本発明は、所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの該要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記監査装置のイベント順序証明監査方法であって、前記証明装置は、前記利用者装置からの前記要求を受信する順序証明要求受信手段と、前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を接続した接続値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む証明書を作成する証明書作成手段と、前記証明書を前記利用者装置に送信する証明書送信手段と、前記利用者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、複数の監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、前記複数の監査用の前記要求を前記順次集約木に割り当てた時点におけるそれぞれの監査用の前記即時補完情報を前記順次集約木から取得し、前記複数の監査用証明書に含める監査用証明書作成手段と、前記監査用証明書を前記監査装置に送信する監査用証明書送信手段と、前記証明書送信後、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、を有し、前記証明装置から、前記複数の監査用証明書を受信する監査用証明書受信ステップと、前記利用者装置から、前記証明書及び前記遅延補完情報を含む前記証明書に対する監査要求を受信する監査要求受信ステップと、受信した複数の監査用証明書の中から、受信した監査要求の第1及び第2の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より生成された時間的順序が後、かつ遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第1の監査用証明書選択ステップと、前記順次集約木の特定のノードに対して、前記第1の監査用証明書選択ステップで選択された監査用証明書に含まれる該ノードの割当値と、前記監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第1の証明書監査ステップと、前記証明書の監査結果を前記利用者装置に送信する監査結果送信ステップと、を有することを特徴とする。

#### 【0019】

請求項9記載の本発明は、請求項8記載の発明において、前記監査用証明書受信ステップは、前記監査用証明書を受信する第1の時刻を時刻提供装置から取得するステップを有し、前記第1の証明書監査ステップは、前記証明書の要求受付が前記第1の時刻よりも時間的に前であることを示す区間時刻証を監査結果に含めることを特徴とする。

#### 【0020】

請求項10記載の本発明は、請求項8又は9記載の発明において、前記証明装置は、前記一定時間間隔終了後に前記監査用証明書作成手段で作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延

補完情報作成手段と、前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、を有し、受信した複数の監査用証明書の中から、受信した監査要求の第1の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より時間的順序が前の監査用証明書を選択する第2の監査用証明書選択ステップと、前記順次集約木の特定のノードに対して、前記監査要求に含まれる該ノードの割当値と、前記第2の監査用証明書選択ステップで選択された監査用証明書及び該監査用証明書の遅延補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第2の証明書監査ステップと、を有することを特徴とする。

#### 【0021】

請求項11記載の本発明は、請求項10記載の発明において、複数の証明書に対する各監査結果と、前記複数の証明書の第1の順次集約木特定情報に基づいて、前記複数の証明書間における要求受付の時間的順序を判定する利用者間順序判定ステップと、を有し、前記監査結果送信ステップは、前記複数の証明書間における要求受付の時間的順序を前記監査結果に含めることを特徴とする。

#### 【0022】

請求項12記載の本発明は、請求項10又は11記載の発明において、前記監査用証明書及び該監査用証明書の遅延補完情報から前記順次集約木のルート値を計算するルート値計算ステップと、電子的に公表された前記順次集約木のルート値と計算されたルート値が一致するか否かの検証を行うルート値検証ステップと、を有することを特徴とする。

#### 【0023】

請求項13記載の本発明は、請求項10乃至12のいずれか1項に記載の発明において、前記第1の監査用証明書選択ステップで選択された監査用証明書及び該監査用証明書の遅延補完情報を前記利用者装置に送信する監査用補完情報送信ステップを有することを特徴とする。

#### 【0024】

請求項14記載の本発明は、請求項10乃至13のいずれか1項に記載の発明において、前記監査用証明書受信ステップは、監査用の前記要求を前記証明装置に送信する第2の時刻を時刻提供装置から取得するステップを有し、前記第2の証明書監査ステップは、前記証明書の要求受付が前記第2の時刻より時間的に後であることを示す区間時刻証を監査結果に含めることを特徴とする。

#### 【0025】

請求項15記載の本発明は、請求項8乃至14のいずれか1項に記載の発明において、前記監査結果は、デジタル署名が施されていることを特徴とする。

#### 【0026】

請求項16記載の本発明は、所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの前記要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記証明装置であって、前記利用者装置からの前記要求を受信する順序証明要求受信手段と、前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を接続した接続値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む証明書を作成する証明書作成手段と、前記証明書を前記利用者装置に送信する証明書送信手段と、前記利用者装置からの前記要求が割り当てられた前記順次集約木のリー

フからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、前記利用者装置からの前記要求を前記順次集約木に割り当てた以後に、監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、監査用証明書を作成するとともに、前記監査用の前記要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、該監査用証明書に含める監査用証明書作成手段と、前記監査用証明書を前記監査装置に送信する監査用証明書送信手段と、前記監査用の要求を前記順次集約木に割り当てた以後に、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、を有することを特徴とする。

#### 【0027】

請求項17記載の本発明は、請求項16記載の発明において、前記証明書の即時補完情報を含むことを特徴とする。

#### 【0028】

請求項18記載の本発明は、請求項16又は17記載の発明において、前記監査用証明書作成手段は、さらに、前記利用者装置からの前記要求を前記順次集約木に割り当てた以前に、監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、監査用証明書を作成するとともに、前記監査用の前記要求を前記順次集約木に割り当てた時点における監査用の前記即時補完情報を前記順次集約木から取得し、該監査用証明書に含める手段を備え、前記一定時間間隔終了後に前記監査用証明書作成手段で作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成手段と、前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、を有することを特徴とする。

#### 【0029】

請求項19記載の本発明は、請求項16乃至18のいずれか1項に記載の発明において、前記順次割当データは、前記要求に含まれるデジタル情報に対して所定の衝突困難一方関数を適用した結果値であることを特徴とする。

#### 【0030】

請求項20記載の本発明は、請求項16乃至19のいずれか1項に記載の発明において、前記証明書は、デジタル署名が施されていることを特徴とする。

#### 【0031】

請求項21記載の本発明は、請求項16乃至20のいずれか1項に記載の発明において、前記一定時間間隔終了後に前記順次集約木のルート値を電子的に公表する電子的情報公表手段を有することを特徴とする。

#### 【0032】

請求項22記載の本発明は、請求項16乃至21のいずれか1項に記載の発明において、前記証明装置は、複数の前記要求を前記順次集約木に順次割り当てたときは、割り当てた時間的順序で、前記複数の要求に対する証明書を送信する手段を有することを特徴とする。

#### 【0033】

請求項23記載の本発明は、所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの該要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記監査装置であって、前記証明装置は、前記利用者装置からの前記要求を受信する順序証明要求受信手段と、前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する

順次割当データ計算手段と、前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を接続した接続値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む証明書を作成する証明書作成手段と、前記証明書を前記利用者装置に送信する証明書送信手段と、前記利用者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、複数の監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、前記複数の監査用の前記要求を前記順次集約木に割り当てた時点におけるそれぞれの監査用の前記即時補完情報を前記順次集約木から取得し、前記複数の監査用証明書に含める監査用証明書作成手段と、前記監査用証明書を前記監査装置に送信する監査用証明書送信手段と、前記証明書送信後、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、を有し、前記証明装置から、前記複数の監査用証明書を受信する監査用証明書受信手段と、前記利用者装置から、前記証明書及び前記遅延補完情報を含む前記証明書に対する監査要求を受信する監査要求受信手段と、受信した複数の監査用証明書の中から、受信した監査要求の第1及び第2の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より生成された時間的順序が後、かつ遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第1の監査用証明書選択手段と、前記順次集約木の特定のノードに対して、前記第1の監査用証明書選択手段で選択された監査用証明書に含まれる該ノードの割当値と、前記監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第1の証明書監査手段と、前記証明書の監査結果を前記利用者装置に送信する監査結果送信手段と、を有することを特徴とする。

#### 【0034】

請求項24記載の本発明は、請求項23記載の発明において、前記監査用証明書受信手段は、前記監査用証明書を受信する第1の時刻を時刻提供装置から取得する手段を有し、前記第1の証明書監査手段は、前記証明書の要求受付が前記第1の時刻よりも時間的に前であることを示す区間時刻証を監査結果に含めることを特徴とする。

#### 【0035】

請求項25記載の本発明は、請求項23又は24記載の発明において、前記証明装置は、前記一定時間間隔終了後に前記監査用証明書作成手段で作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成手段と、前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、を有し、受信した複数の監査用証明書の中から、受信した監査要求の第1の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より時間的順序が前の監査用証明書を選択する第2の監査用証明書選択手段と、前記順次集約木の特定のノードに対して、前記監査要求に含まれる該ノードの割当値と、前記第2の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明す

る第2の証明書監査手段と、を有することを特徴とする。

【0036】

請求項26記載の本発明は、請求項25記載の発明において、複数の証明書に対する各監査結果と、前記複数の証明書の第1の順次集約木特定情報に基づいて、前記複数の証明書間における要求受付の時間的順序を判定する利用者間順序判定手段と、を有し、前記監査結果送信手段は、前記複数の証明書間における要求受付の時間的順序を前記監査結果に含めることを特徴とする。

【0037】

請求項27記載の本発明は、請求項25又は26記載の発明において、前記監査用証明書及び該監査用証明書の遅延補完情報から前記順次集約木のルート値を計算するルート値計算手段と、電子的に公表された前記順次集約木のルート値と計算されたルート値が一致するか否かの検証を行うルート値検証手段と、を有することを特徴とする。

【0038】

請求項28記載の本発明は、請求項25乃至27のいずれか1項に記載の発明において、前記第1の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延補完情報を前記利用者装置に送信する監査用補完情報送信手段を有することを特徴とする。

【0039】

請求項29記載の本発明は、請求項25乃至28のいずれか1項に記載の発明において、前記監査用証明書受信手段は、監査用の前記要求を前記証明装置に送信する第2の時刻を時刻提供装置から取得する手段を有し、前記第2の証明書監査手段は、前記証明書の要求受付が前記第2の時刻より時間的に後であることを示す区間時刻証を監査結果に含めることを特徴とする。

【0040】

請求項30記載の本発明は、請求項25乃至29のいずれか1項に記載の発明において、前記監査結果は、デジタル署名が施されていることを特徴とする。

【0041】

請求項31記載の本発明は、請求項1乃至7のいずれか1項に記載のイベント順序証明方法の各ステップを前記証明装置に実行させるイベント順序証明プログラムであることを特徴とする。

【0042】

請求項32記載の本発明は、請求項8乃至15のいずれか1項に記載のイベント順序証明監査方法の各ステップを前記証明監査装置に実行させるイベント順序証明監査プログラムであることを特徴とする。

【0043】

請求項33記載の本発明は、所定のデジタル情報の生成を伴うイベントに対して時間的順序の証明を要求する利用者装置と、前記利用者装置からの前記要求に対する証明書を作成する証明装置と、前記証明書の真偽を監査する監査装置とが、それぞれ通信ネットワークを介して相互に接続されているイベント順序証明システムにおける前記利用者装置のためのイベント順序証明検証プログラムであって、前記証明装置は、前記利用者装置からの前記要求を受信する順序証明要求受信手段と、前記要求に含まれるデジタル情報から予め定めた手順に従って順次割当データを作成する順次割当データ計算手段と、前記順次割当データを時刻順に有向木のリーフに左から順次割り当て、一定時間間隔ごとに1つの集約木が生成される順次集約木において、同一の親を有する複数の子に割り当てられたそれぞれの割当値を接続した接続値に所定の衝突困難一方向関数を適用した結果値を前記親の割当値とする計算方法により、計算可能なノードの割当値を計算するとともに、前記一定時間間隔終了後に前記順次集約木のルートに割り当てるルート値を計算する順序証明要求集約手段と、前記順次割当データ、並びに前記順次割当データが割り当てられた順次集約木及び該順次集約木のリーフを特定する第1の順次集約木特定情報を含む証明書を作成する証明書作成手段と、前記証明書を前記利用者装置に送信する証明書送信手段と、前記利用

者装置からの前記要求が割り当てられた前記順次集約木のリーフからルート値を計算するのに必要な他のノードに関する情報を前記証明書の補完情報と定義し、該補完情報のうち、前記利用者装置からの前記要求を前記順次集約木に割り当てた時点において取得可能な補完情報を即時補完情報と定義すると、複数の監査用の前記要求を前記順次集約木に割り当て、前記証明書と同一の作成方法により、複数の監査用証明書を作成するとともに、前記複数の監査用の前記要求を前記順次集約木に割り当てた時点におけるそれぞれの監査用の前記即時補完情報を前記順次集約木から取得し、前記複数の監査用証明書に含める監査用証明書作成手段と、前記監査用証明書を前記監査装置に送信する監査用証明書送信手段と、前記証明書送信後、前記利用者装置からの前記証明書の補完情報の要求を受信する補完情報要求受信手段と、前記補完情報の要求が割り当てられた前記順次集約木及び前記順次集約木のリーフを特定する第2の順次集約木特定情報、及び前記補完情報の要求を割り当てた時点において取得可能な補完情報を前記順次集約木から取得し、遅延補完情報とする遅延補完情報作成手段と、前記遅延補完情報を前記利用者装置に送信する遅延補完情報送信手段と、を有し、前記監査装置は、前記証明装置から、前記複数の監査用証明書を受信する監査用証明書受信手段と、前記利用者装置から、前記証明書及び前記遅延補完情報を含む前記証明書に対する監査要求を受信する監査要求受信手段と、受信した複数の監査用証明書の中から、受信した監査要求の第1及び第2の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より生成された時間的順序が後、かつ遅延補完情報より生成された時間的順序が前である監査用証明書を選択する第1の監査用証明書選択手段と、前記順次集約木の特定のノードに対して、前記第1の監査用証明書選択手段で選択された監査用証明書に含まれる該ノードの割当値と、前記監査要求から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時間的前後を証明する第1の証明書監査手段と、前記証明書の監査結果を前記利用者装置に送信する監査結果送信手段と、を有し、前記要求を前記証明装置に送信する順序証明要求送信ステップと、前記証明装置から、前記証明書を受信する証明書受信ステップと、前記証明書の補完情報の要求を前記証明装置に送信する補完情報要求送信ステップと、前記証明装置から、前記補完情報を受信する補完情報受信ステップと、前記監査要求を前記監査装置に送信する監査要求送信ステップと、前記監査結果を受信する監査結果受信ステップと、を前記利用者装置に実行させることを特徴とする。

#### 【0044】

請求項34記載の本発明は、請求項33記載の発明において、前記監査装置の前記監査用証明書受信手段は、前記監査用証明書を受信する第1の時刻を時刻提供装置から取得する手段を有し、前記第1の証明書監査手段は、前記証明書の要求受付が前記第1の時刻よりも時間的に前であることを示す区間時刻証を監査結果に含め、前記要求を前記証明装置に送信する時点の第3の時刻を前記時刻提供装置から取得し、該第3の時刻を所定の手順に従って計算した値を前記要求に含める順序証明要求作成ステップを前記利用者装置に実行させることを特徴とする。

#### 【0045】

請求項35記載の本発明は、請求項33又は34記載の発明において、前記証明装置は、前記一定時間間隔終了後に前記監査用証明書作成手段で作成された各監査用証明書の補完情報すべてを前記順次集約木から取得し、各監査用証明書の遅延補完情報とする監査用遅延補完情報作成手段と、前記各監査用証明書の遅延補完情報を前記監査装置に送信する監査用遅延補完情報送信手段と、を有し、前記監査装置は、受信した複数の監査用証明書の中から、受信した監査要求の第1の順次集約木特定情報に基づいて、前記監査要求に含まれる証明書より時間的順序が前の監査用証明書を選択する第2の監査用証明書選択手段と、前記順次集約木の特定のノードに対して、前記監査要求に含まれる該ノードの割当値と、前記第2の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延補完情報から計算された該ノードの割当値が一致するか否かの検証に基づいて、前記証明書の正当性を監査し、前記証明書の要求受付と選択された監査用証明書の要求受付の時

間的前後を証明する第2の証明書監査手段と、を有することを特徴とする。

【0046】

請求項36記載の本発明は、請求項35記載の発明において、前記監査装置は、複数の証明書に対する各監査結果と、前記複数の証明書の第1の順次集約木特定情報に基づいて、前記複数の証明書間における要求受付の時間的順序を判定する利用者間順序判定手段を有し、前記監査結果送信手段は、前記複数の証明書間における要求受付の時間的順序を前記監査結果に含め、前記監査要求は、他の証明書との時間的順序の判定要求を含むことを特徴とする。

【0047】

請求項37記載の本発明は、請求項35記載の発明において、前記監査装置は、前記第1の監査用証明書選択手段で選択された監査用証明書及び該監査用証明書の遅延補完情報を前記利用者装置に送信する監査用補完情報送信手段を有し、前記監査装置から送信された監査用証明書及び該監査用証明書の遅延補完情報を受信するステップを前記利用者装置に実行させることを特徴とする。

【0048】

請求項38記載の本発明は、請求項34乃至37のいずれか1項に記載の発明において、前記監査用証明書受信手段は、監査用の前記要求を前記証明装置に送信する第2の時刻を時刻提供装置から取得する手段を有し、第2の証明書監査手段は、前記証明書の要求受付が前記第2の時刻より時間的に後であることを示す区間時刻証を監査結果に含め、前記要求を前記証明装置に送信する時点の第3の時刻を前記時刻提供装置から取得し、該第3の時刻を所定の手順に従って計算した値を前記要求に含める順序証明要求作成ステップを前記利用者装置に実行させることを特徴とする。

【0049】

請求項39記載の本発明は、請求項33乃至38のいずれか1項に記載の発明において、前記証明装置から受信した証明書、及び前記一定時間間隔終了後に取得した該証明書の補完情報すべてから、前記順次集約木のルート値を計算するルート値計算ステップと、前記一定時間間隔終了後に電子的に公表された前記順次集約木のルート値と計算されたルート値が一致するか否かの検証を行うルート値検証ステップと、を前記利用者装置に実行させることを特徴とする。

【0050】

請求項40記載の本発明は、請求項34又は38記載のイベント順序証明検証プログラムを実行する利用者装置が前記要求に付した時刻を検証するコンピュータが読み取り可能なイベント時刻検証プログラムであって、前記監査結果を取得する監査結果取得ステップと、前記監査結果に対応する前記要求を取得する順序証明要求取得ステップと、前記第3の時刻と、前記第1又は第2の時刻のうち少なくとも1以上との時間差に基づいて、前記第3の時刻の正当性を判定する時刻検証ステップと、前記判定結果を出力するステップと、前記コンピュータに実行させることを特徴とする。

【発明の効果】

【0051】

本発明によれば、木構造を用いてイベント順序を証明するイベント順序証明システムにおいて、イベント順序証明要求をまとめた公表データを用いなくとも、イベント順序証明機関から発行されたイベント順序受理証明書の検証を行うことができる。

【0052】

この結果、公表期間の途中であっても、受け取ったイベント順序受理証明書の正当性を検証することができ、利用者の利便性の向上を図ることができる。また、イベント順序証明機関に障害が発生しても、障害に強いイベント順序証明システムを構築することができる。

【発明を実施するための最良の形態】

【0053】

以下、本発明の実施の形態を図面を用いて説明する。

#### 【0054】

##### <第1の実施の形態>

##### (1-1. システム構成)

図1は、本発明の第1の実施の形態に係るイベント順序証明システム100のシステム構成図である。同図に示すイベント順序証明システム100は、イベント順序証明装置（以下、証明装置という）1、複数のイベント順序証明利用者装置（以下、利用者装置という）2i（ $i=a, b, \dots, n$ ）、証明装置1が発行したイベント順序受理証明書（以下、受理証明書という）の監査を行うイベント順序証明監査装置（以下、監査装置という）3、及び、以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成されるコンピュータネットワーク4を備えており、証明装置1が利用者装置2iからのイベント順序証明要求（以下、証明要求という）に応じて、受理証明書を発行し、利用者装置2iに返信すると共に、受理証明書に疑義が生じた場合には、利用者装置2iは、証明装置1が公表したデータ又は監査装置3による監査結果によって受理証明書を検証することができるようになっている。

#### 【0055】

尚、図1に示すイベント順序証明システム100のシステム構成は機能が同一であればその形態は問わないものであり、その物理的構成は種々考えられるものである。例えば、図2に示すように、利用者装置2iの代わりに、イベント順序証明利用者検証装置（以下、利用者検証装置という）6iが受理証明書の検証を行うようにしてもよいし、証明装置1の代わりに電子的情報公表装置5が証明装置1から公表データをもらい、公開するようにしてもよい。また、コンピュータネットワーク4は、郵便など他の通信手段に置き換えることも可能である。尚、以下においては、図1のシステム構成のもとに構成及び動作を説明する。

#### 【0056】

証明装置1は、コンピュータネットワーク4を介して利用者装置2i及び監査装置3とデータの送受信を行う送受信部11、利用者装置2iからの証明要求として送信されたデジタル・データを順次集約木を用いてまとめるイベント順序証明要求集約部12、受理証明書を作成するイベント順序証明作成部13、監査装置3に送信する監査情報を作成する監査情報作成部14、利用者装置2iからの補完データ要求に応じて補完データを取得する補完データ取得部15、証明装置1が一定期間に発行した複数の受理証明書の内容を連結したデータに対して高強度デジタル署名をする高強度デジタル署名作成部16、高強度デジタル署名されたデータを電子的に公表する電子的情報公表部17、及び受理証明書をはじめとするイベント順序証明に関する情報を記憶する記憶部18を有する構成である。

#### 【0057】

上述したように、イベント順序証明要求集約部12は、順次集約木を用いてイベント順序証明要求をまとめるが、この順次集約木について図3を用いて説明する。図3に示す順次集約木は、一定期間（例えば1週間など証明装置1が取り纏めデータを公表するサイクル、以下、順次集約期間という）において完成される集約木であって、利用者装置2iからの証明要求に含まれるデジタル・データの全部あるいは一部から所定の順次割当データ計算手順に従って生成されたデジタル・データ（これを順次割当データと呼ぶ；例えば、証明要求に含まれるデジタル・データのハッシュ値）を経時的に順次リーフに左側から割り当てるようにしている。

#### 【0058】

順次集約木の各ノード（リーフを除く）に割り当てられる値の計算方法は、以下の通りである。順次集約木の親の割当値は、左側の子の割当値 $H'$ と右側の子の割当値 $H''$ を接続（ビット列とビット列の結合）し、所定の衝突困難一方向ハッシュ関数 $h$ を適用した結果であるハッシュ値を計算することにより求められるものであり、これを $h(H' || H'')$ と表す。このようにして下位のレベルの割当値から上位のレベルの割当値を計算して、最終的に最上位のレベル（ルート）の割当値（ルート値）を求める。



#### 【0059】

以下においては、図3に示すように、16のリーフを有する順次集約木の場合について説明する。尚、順次集約木リーフの数や高さは、順次集約期間が終了するまで確定しない。また、順次集約木においては、リーフへの値の割当は左から順次行われ、レベルが0より大きいノード（即ちリーフではないノード）に対する値の割当は、それが可能になったときにインクリメンタルに行われる。従って、図3の同一の縦線上にある複数のノードに対しては、値の割当が同一の処理単位の中ではほぼ同時に行われる。

ここで、順次集約木のレベル $j$ 、番号（インデックスともいう） $i$ のノードを $(j, i)$ で表し、ノード $(j, i)$ の割当値を $V(j, i)$ と表して、図3に示す具体例を説明する。

#### 【0060】

今、順次割当データがノード $(0, 5)$ に割り当てられたとき、即ち、順次集約木リーフに割り当てるハッシュ値が $V(0, 5)$ であるとき、このハッシュ値 $V(0, 5)$ からルート値（ $=V(4, 0)$ ）を求めるには、 $V(0, 5)$ に $V(0, 4)$ を左から接続して、ハッシュ値 $h1'$ を計算し、該ハッシュ値 $h1'$ に $V(1, 3)$ を右側から接続してハッシュ値 $h2'$ を計算し、該ハッシュ値 $h2'$ に $V(2, 0)$ を左側から接続してハッシュ値 $h3'$ を計算し、さらに該ハッシュ値 $h3'$ に $V(3, 1)$ を右側から接続してハッシュ値（ $=V(4, 0)$ ）を計算すればよい。このような手順により $V(0, 5)$ とそれを補完するデータ（ここでは $V(0, 4)$ 、 $V(1, 3)$ 、 $V(2, 0)$ 、 $V(3, 1)$ ）からルート値が計算できるとき、 $V(0, 5)$ はハッシュ関数 $h$ によりルート値にリンクするという。また、順次集約木における $V(0, 5)$ の補完データ（以下、順次集約補完データという）は、

【 $(V(0, 4), L)$ 、 $(V(1, 3), R)$ 、 $(V(2, 0), L)$ 、 $(V(3, 1), R)$ 】

となる。ここで、 $L$ 及び $R$ は、各々、2つのデジタル・データを接続する際に左から接続こと、及び右から接続することを表す。

#### 【0061】

イベント順序証明作成部13は、図4に示すような受理証明書 $EOC(y)$ を作成し、利用者装置2iに送信するようになっている。同図によれば、受理証明書 $EOC(y)$ は、利用者から送付されたデジタル・データ $y$ 、上述した順次割当データ計算手順によりデジタル・データ $y$ から計算された順次割当データ $z$ 、順次割当データ $z$ が割り当てられた順次集約木を一意に特定できる順次集約木番号、順次割当データ $z$ が割り当てられた順次集約木リーフを一意に特定できる順次集約木リーフ番号、およびその時点で取得できる順次集約補完データの一部（これを即時補完データという） $HK$ を含むように構成されている。このうち、即時補完データ $HK$ については省くことも可能である。

#### 【0062】

また、同図によれば、イベント受理証明書 $EOC(y)$ には、証明装置1が予め用意しておいた公開鍵暗号方式キー・ペアのうちの秘密鍵（署名用秘密鍵）を用いてデジタル署名をつけて送信してもよい。この場合、当該公開鍵暗号方式キー・ペアのうちの公開鍵は公開鍵暗号基盤などを用いて利用者装置2iからアクセス可能になっているものとする。

#### 【0063】

尚、当該の受理証明書 $EOC(y)$ 発行後に取得できる順次集約補完データを遅延補完データという。即ち、受理証明書 $EOC(y)$ が作成される段階においては、即時補完データだけが利用者装置2iに送信されるものであり、遅延補完データは、当該の受理証明書 $EOC(y)$ 発行後に要求された場合等に利用者装置2iに送信されるものである。例えば、図3の具体例においては、ノード $(0, 5)$ にとって、ノード割当値 $V(2, 0)$ 、ノード割当値 $V(0, 4)$ は即時補完データであるが、ノード割当値 $V(1, 3)$ 、ノード割当値 $V(3, 1)$ はノード $(0, 15)$ が割り当てられた時点以降に取得可能な遅延補完データである。以下では、順次集約木リーフ番号 $i$ に対して、 $V(0, i)$ のことを短く $V(i)$ と書くこともある。

#### 【0064】

補完データ取得部14は、利用者装置2iから上述した遅延補完データの要求があったとき、当該時点に関する情報（当該要求が割り当てられた順次集約木番号、順次集約木リーフ番号）、及びその時点で確定している順次集約補完データ（位置情報、割当値）の全てを利用者装置2iに返送するようになっている。

#### 【0065】

ここで、図5を参照して、順次集約補完データの内容について詳しく説明する。

#### 【0066】

順次集約木の1つのリーフ  $l$  に対する、 $l$  より右に位置するもう一つのリーフ  $l'$  における補完データ  $CToken(l, l')$  は次のように定義される。

#### 【0067】

リーフ  $l$  から順次集約木のルートに至るパスを  $l$  のルート・パスと呼び、 $l$  のルート・パスに属するルート以外のノードの兄弟ノードからなるノードの並びを  $l$  の認証パスと呼ぶ（認証パスの詳細な定義は後で与える）。認証パスの要素の内、 $l$  より右に位置するリーフ  $l'$  の割り当て値が確定した時点において割当値が確定している要素の列を  $authPathD(l, l')$  とし、これを  $l'$  における  $l$  に対する認証パスと呼ぶ。この列に割当値の情報を付加したものを  $authPathDV(l, l')$  とし、これを  $l'$  における  $l$  に対する値付認証パスと呼ぶ。

#### 【0068】

以上から、 $authPathDV(l, l')$  は、受理証明書  $EOC(y)$  に含まれていなかった情報を含めて、補完データ  $CToken(l, l')$  を構成するようになっている。

#### 【0069】

尚、 $l'$  が  $l$  の属する順次集約木  $SBT$  の生成期間（順次集約期間）の終了後に生成される次の順次集約木  $SBT'$  のリーフであるときにも、 $authPathDV(l, l')$  には順次集約木  $SBT$  についての情報のみが含まれる。このとき、 $CToken(l, l')$  は、 $l$  時点で受信したイベント受理証明書  $EOC(y)$  と組み合わせることにより、当該の順次集約期間における順次集約木のルート値を計算するのに十分な情報をふくんでいる。

#### 【0070】

例えば、図5において、 $CToken(l, l')$  は  $a1$  の位置情報  $(0, 3)$  とその割当値  $V(a1)$  の組  $((0, 3), V(a1))$ 、及び  $a2$  の位置情報  $(2, 1)$  とその割当値  $V(a2)$  の組  $((2, 1), V(a2))$  からなる列  $[((0, 3), V(a1)), ((2, 1), V(a2))]$  となる。

#### 【0071】

以下では、受理証明書に含まれる順次集約木の割当て値と組み合わせることにより前記順次集約木のルート値を計算できるような補完データを該受理証明書の完全補完データと定義し、上記割当て値および受理証明書に含まれる即時の補完データと組み合わせることにより、前記順次集約木のルート値を計算できるような補完データを完全遅延補完データと呼ぶ。

#### 【0072】

監査情報作成部14は、監査情報を順次集約木から取得して監査装置3に送信するものであり、より詳しくは、監査情報とは、順次集約木リーフに設けられた監査点において以下に定義するように生成される監査用イベント順序受理証明書（以下、監査用受理証明書という）から構成される。ここで、監査点とは、監査装置3からの監査用イベント順序証明要求（以下、監査用証明要求という）が割当てられた順次集約二分木のリーフをいう。

#### 【0073】

尚、図3の具体例においては、監査点は1つしか設けられていないが、所定のアルゴリズムに従って複数設けてよいのは勿論であり、また、証明要求に対する受理証明書に対して後述するような監査を行うためには、監査点は、該証明要求に対応するリーフ（図3の具体例においては、ノード  $(0, 5)$ ）に等しいか或いはそれより右側のリーフ（時間的に後）に割り当てられていればどこに設けていてもよいものである。

#### 【0074】

監査用受理証明書の形式は、利用者装置2に返送する受理証明書と同一である。尚、順次割当データを計算するための元となるデジタル・データ  $y$  は、監査装置3から証明装置1に監査用証明要求として送付されたものであってもよいし、当該証明装置1において、当該の監査装置2に対して予め定められた何らかの手順に従って生成してもよい。また、こ

のような手順としては、前以て定められた何らかの手順に従って監査用受理証明書におけるイベント順序証明の対象となるデジタル文書を作成し、該デジタル文書に対して前以て定めたハッシュ関数を適用した結果であるハッシュ値を順次割当データを計算するための元となるデジタル・データとする方式を採用してもよい。

#### 【0075】

利用者装置2iは、コンピュータネットワーク4を介して証明装置1および監査装置3とデータを送受信する送受信部21、所定のデジタル・データを含む証明要求を行うイベント順序証明要求部22、要求時点において取得可能な受理証明書に対する補完データを要求する補完データ要求部23、受理証明書を検証するイベント順序証明検証部24、受理証明書をはじめとするイベント順序証明に関する情報を記憶する記憶部25を有する構成である。

#### 【0076】

ここで、イベント順序証明検証部24は、受理証明書に対して以下の検証機能を備える。

#### 【0077】

まず、受理証明書にデジタル署名が含まれる場合には、該デジタル署名に対するデジタル署名検証を行う第0の検証機能を備える。

#### 【0078】

また、証明装置1から高強度デジタル署名を付すこと等により真正性を保証して公表される公表情報に、受理証明書に含まれる順次割当データがハッシュ関数を介してリンクすることを検証する第1の検証機能を備える。

#### 【0079】

さらに、以下に記述するように、証明装置1からの公表情報が公開される前であっても、監査装置3を利用することにより、受理証明書の正当性を検証する第2の検証機能を備える。

#### 【0080】

監査装置3は、コンピュータネットワーク4を介して証明装置1および利用者装置2iとデータを送受信する送受信部31、利用者装置2iからある受理証明書の監査要求を受けた際には、利用者装置2iから送信された監査要求情報および自己の監査情報を用いて受理証明書の検証を行い、その結果を利用者装置2iに返信するイベント順序証明監査部32、及び監査用受理証明書をはじめとする監査情報を記憶する記憶部33を有する構成である。

#### 【0081】

ここで、イベント順序証明検証部32の機能について、図3の具体例を用いて説明する。図3の具体例においては、(0,10)が監査点となっているので、この時点において監査装置3が受け取っている監査情報は、上述した通り、V(3,0)およびV(1,4)である。一方、利用者装置2iは、監査要求情報として、V(0,5)及び順次集約補完データであるV(0,4)、V(1,3)、およびV(2,0)を送信するものである。これは、利用者装置2iが検証を求める時点（即ち、受理証明書が発行された(0,5)の時点より後刻である監査点(0,10)の時点以降）においては、即時補完データに含まれていなかったV(1,3)も証明装置1から取得することが可能であるので、V(1,3)を遅延補完データとして利用者装置2iが証明装置1から取得し、監査要求情報に含めたものである。そして、イベント順序証明検証部32は、自己が有している監査情報V(3,0)が、利用者装置2iから送信された監査要求情報から計算されたV(3,0)と一致するか否かを検証するものである。

#### 【0082】

尚、以後においては、利用者装置2iから送信された証明要求から作成された順次割当データが割り当てられた順次集約木リーフをユーザ点と呼び、監査装置3から送信された監査用証明要求から作成された順次割当データが割り当てられた順次集約木リーフを監査点と呼ぶ。

#### 【0083】

ここで、比較検証の対象となる順次集約木のノード（図3の具体例においては、(3,0)）を以後、認証点とよぶ。尚、一般に、あるユーザ点の番号が監査点の番号より小さい場合、認証点のラベル（割当値）は監査情報に含まれており、また、監査点におけるイベント

順序証明処理が終了した時点以降において、利用者装置2iが受信できる遅延補完データから計算できるラベルには、認証点のラベルが含まれるので、順次集約木においてユーザ点、監査点、遅延補完データを要求した点が左からこの順序に位置している場合には、上記検証は、常に実施可能なものであるが、この理由に関しては後述する(後述の順次集約木の性質2の項目(3)を参照)。

#### 【0084】

即ち、上記の手順により利用者装置2iがある受理証明書に対する第2の検証を監査装置3に依頼して実行するには、該受理証明書の証明要求が割り当てられたリーフ $\tau$ と、該イベント受理証明書に対する遅延補完データ要求が割り当てられたリーフ $\tau'$ の間( $\tau$ と $\tau'$ も含む)に監査装置3の監査点が存在する必要がある。

#### 【0085】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置(CPU: Central Processing Unit)、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置(メモリ)、ハードディスク(HD)等の電源断時にもデータを記憶し続けることが出来る2次記憶装置を有する電子的な装置から構成されている。このうち、証明装置1のイベント順序証明要求集約部12、イベント順序証明作成部13、監査情報作成部14、補完データ取得部15、デジタル署名作成部16及び電子的情報公表部17、利用者装置2iのイベント順序証明要求部22、補完データ要求部23及びイベント順序証明検証部24、並びに監査装置3のイベント順序証明監査部32の処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、証明装置1の記憶部18、利用者装置2iの記憶部25及び監査装置3の記憶部33は、上記主記憶装置あるいは2次記憶装置の機能を備えたものである。

#### 【0086】

また、本実施の形態に係る各種処理を実行するプログラムは、前述した主記憶装置または2次記憶装置に格納されているものである。そして、このプログラムは、ハードディスク、フレキシブルディスク、CD-ROM、MO、DVD-ROMなどのコンピュータ読み取り可能な記録媒体に記録することも、通信ネットワークを介して配信することも可能である。

#### 【0087】

##### (1-2. システム動作)

次に、以上の構成を有するイベント順序証明システム100におけるイベント順序証明方法、およびイベント順序証明検証方法を図6乃至8を用いて説明する。ここで、図6は、1つの順次集約期間において証明装置1が受理証明書及び監査用受理証明書を作成する動作を説明するシーケンス図であり、図7は、利用者装置2iが受理証明書に対して第1の検証を行う動作を説明するフローチャートであり、図8は、利用者装置2iが受理証明書に対して第2の検証を行う動作を説明するシーケンス図である。

#### 【0088】

まず、図6を参照して、イベント順序証明方法について説明する。

#### 【0089】

利用者装置2iが証明装置1にデジタル・データ $y$ を含む証明要求を送信すると、証明装置1は送受信部11を介して、該デジタル・データ $y$ を含む証明要求を受信する(ステップS10、S20)。

次に、イベント順序証明要求集約部12が、デジタル・データ $y$ を入力の一部あるいは全部として順次割当データ $z$ を計算し、該順次割当データ $z$ を順次集約木リーフに割り当て、インクリメンタルに順次集約木を構成していくとともに、イベント順序証明作成部13が、受理証明書E0C( $y$ )を作成し、送受信部11を介して利用者装置2iに受理証明書E0C( $y$ )を送信する(ステップS30、S40、S50)。

#### 【0090】

これにより、利用者装置2iは、受理証明書E0C( $y$ )を取得することができる(ステップS60)。尚、受理証明書E0C( $y$ )には、この時点において取得できる即時補完データを含

めることにしてよいが、遅延補完データは含まれていない。

【0091】

同様にして、監査装置3も監査用証明要求を送信すると、証明装置1は送受信部11を介して、監査用証明要求を受信する(ステップS70、S80)。

【0092】

次に、イベント順序証明要求集約部12が、監査用証明要求から計算された監査用順次割当データを順次集約木リーフに割り当てて、インクリメンタルに順次集約木を構成していくとともに、監査情報作成部13は、監査用受理証明書を作成し、送受信部11を介して監査装置3に監査用受理証明書を送信する(ステップS90、S100、S110)。

【0093】

これにより、監査装置3は、監査用受理証明書を取得することができる(ステップS120)。

【0094】

次に、利用者装置2iは、取得した受理証明に対する遅延補完データ要求を証明装置1に送信すると、証明装置1は送受信部11を介して、該遅延補完データ要求を受信する(ステップS130、S140)。

【0095】

次いで、証明装置1の補完データ取得部15は、その時点で取得可能な上記受理証明書に対する補完データを取得し、遅延補完データとして送受信部11を介して利用者装置2iに送信する(ステップS150、S160)。

【0096】

これにより、利用者装置2iは、監査に必要な遅延補完データを取得することができる(ステップS170)。

【0097】

そして、順次集約のための一定期間(順次集約期間)内においては、上述した証明装置1の動作は繰り返され、順次集約期間が終了すると、順次集約木のルート値を計算し、電子的情報公表部17は、このルート値を電子的に公表する(ステップS180、S190、S200)。この際、該情報の真正性を保証するため、高強度デジタル署名作成部16を用いて高強度のデジタル署名を付した公表情報を公開してもよい。

【0098】

尚、図6に示すイベント順序証明方法においては、監査装置3の方から証明装置1に監査情報要求を送信し、これに応じて証明装置1が監査装置3に監査情報を送信する方式であったが、これとは異なり、証明装置1が監査装置3に監査情報を自動的に送信するような方式であってもよい。

【0099】

次に、図7を参照しながら、電子的に公表された公表情報を用いたイベント順序証明検証方法について説明する。これは、利用者装置2iの第1の検証機能に相当するものである。

【0100】

まず、利用者装置2iは、自己が証明装置1に証明要求として送信したデジタル・データ $y$ 、並びに受信した受理証明書 $EOC(y)$ 及び遅延補完データに含まれている順次集約補完データ(この時点においては、すべての順次集約補完データを取得可能である)から順次集約木のルート値 $RH_{cal}$ を計算する(ステップS310)。

次に、高強度のデジタル署名を付して電子的に公表されている同一順次集約期間のルート値 $RH$ を取得し、このルート値 $RH$ が、計算したルート値 $RH_{cal}$ に一致するか否かを検証する(ステップS320、S330)。

【0101】

以上の検証において、検証に成功すれば、受理証明書が改ざんされていないことを確認することができる(ステップS340)。一方、検証に失敗すれば、受理証明書が改ざんされていることを確認することができる(ステップS350)。これにより、高強度のデジタ

ル署名を付すなどの手段により真正性を保証しながら電子的に公表された後においては、公表された情報を利用して、証明装置1が発行した受理証明書が、当該の順次集約期間において、受理証明書に含まれる元デジタル・データに対して、受理証明書に含まれる順次集約木リーフ番号で識別される順番において発行されたものであることを確実に検証することができる。

#### 【0102】

次に、図8を参照しながら、監査装置3を用いたイベント順序証明検証方法について説明する。これは、利用者装置2iの第2の検証機能に相当するものである。

#### 【0103】

利用者装置2iは、監査要求の前に検証の対象となる受理証明書の遅延補完データを証明装置1に要求する（ステップS410）。この要求を証明装置1が送受信部11を介して受信すると、補完データ取得部15は、受理証明書に即時補完データが含まれる場合には、この時点において取得できる遅延補完データの全てから即時補完データを除いたものからなる遅延補完データを、受理証明書に即時補完データが含まれない場合には、この時点において取得できる遅延補完データの全てを取得し、送受信部11を介して利用者装置2iに送信する（ステップS420、S430、S440）。これにより、利用者装置2iは、補完データを取得するので、イベント順序証明検証部24は、これに既に受け取っている受理証明書を加えた監査要求情報を監査装置3に送信する（ステップS450、S460）。

#### 【0104】

次に、監査装置3が監査要求情報を送受信部31を介して受信すると、イベント順序証明監査部32は、既に自分が受信した監査用受理証明書が割当てられた順次集約木のリーフの中で、受信したこの監査要求情報に含まれる受理証明書が割当てられた順次集約木リーフ $\tau$ とその遅延補完情報に含まれるリーフ $\tau'$ の間にある監査点 $\alpha$ を計算する（ステップS470、S480）。続いて、監査要求情報から $\tau$ の $\alpha$ による認証点を計算し、該認証点の割当値 $A_{cal}$ を計算する（ステップS490）。一方、イベント順序証明検証部32は、監査情報として既に受け取っているこの認証点の割当値 $A$ を記憶部33から取得して、この認証点の割当値 $A$ が、計算により求めた認証点の割当値 $A_{cal}$ に一致するか否かを検証する（ステップS500、S510）。1

以上の検証において、検証に成功すれば、受理証明書が改ざんされていないことを確認することができる（ステップS520）。一方、検証に失敗すれば、受理証明書が改ざんされていることを確認することができる（ステップS530）。そして、イベント順序証明監査部32は、この監査結果を送受信部31を介して利用者装置2iに送信し、利用者装置2iは、監査結果を受信する（ステップS540、S550）。

#### 【0105】

これにより、利用者装置2iは、電子的公表機関を介した公表前においても、証明装置1が発行した受理証明書が当該の順次集約期間において、受理証明書に含まれる元デジタル・データに対して、受理証明書に含まれる順次集約木リーフ番号で識別される順番において発行されたものであることを確実に検証することができる。尚、上記監査結果に監査点 $\alpha$ の識別子を含めてもよい。この場合においては、利用者装置2iは、上記監査を要求した受理証明書に対応する証明要求の登録が、監査点 $\alpha$ に対応する監査用証明要求の登録より前であったことの保証を監査装置3から確実に得ることができる。

#### 【0106】

なお、ステップS540の監査結果の送信に際しては、監査装置3が受信した補完データを含む部分に対して、証明監査装置3が持つ署名用秘密鍵を用いてデジタル署名を付して、該デジタル署名を含めた検証結果を構成し、利用者装置2iに送信するようにしてもよい。これにより、監査装置3によるデジタル署名が信用されるという前提の下で、順次集約木のルート値に対する有効なデジタル署名が入手できない場合であっても、利用者装置2iを利用する利用者は、上記受理証明書によるイベント順序証明の正当性を客観的に第三者に証明することができるようになる。

#### 【0107】

(1-3. イベント順序監査方法)

次に、上述した第2の検証である監査装置3を用いたイベント順序証明検証方法について、より詳しく説明する。

【0108】

尚、以下では、時刻の原点として、イベント順序証明システム100のサービス開始時点を取り、時間を計る単位として一つの値（例えば1秒、1ミリ秒等）を定め、時刻を上記原点から上記の時間の単位で計った整数で表現するものとする。

【0109】

また、イベント順序証明検証方法を説明するための幾つかの予備定義を与える。

【0110】

順次集約木SBTにおいて、1つのノード $p$ はレベル $j$ とレベル内の番号 $i$ で識別されるが、ノード $p$ のレベルと番号を各々  $level(p)$ 、 $index(p)$  と書く。

【0111】

また、順次集約木リーフ番号 $i$ で識別される順次集約木SBTのリーフを  $leaf(SBT, i)$ 、 $leaf(SBT, i)$  に順次割当値を割り当てる元となった証明要求を受付けて該リーフに割当値を割り当てる一連の処理を該リーフに対する処理ラウンドと言い  $round(SBT, i)$  と表す。文脈からどの順次集約木について論じているか明らかなき場合は、単に  $leaf(i)$ 、 $round(i)$  と記すこともある。

【0112】

順次集約木には、生成された順に0から始まる識別番号を付与し、これを順次集約木番号という。 $n$ 番目の順次集約木リーフの数を  $N(n)$  とおく。

【0113】

各受理証明書に対しては、順次集約木番号 $n$ と順次集約木リーフ番号 $i$ が付与され、該受理証明書が発行された順次集約木リーフをそれら2つの番号の組で指定することができる。このような組を拡張リーフ識別子と呼ぶ。2つの拡張リーフ識別子  $\nu_1 = (n_1, i_1)$ 、 $\nu_2 = (n_2, i_2)$  の間の順序を辞書式順序を用いて定義する。即ち、 $\nu_1 < \nu_2$  とは、 $n_1 < n_2$ 、または  $n_1 = n_2$  かつ  $i_1 < i_2$  のことと定義する。また  $\nu_1 \leq \nu_2$  とは、 $\nu_1 < \nu_2$  または  $\nu_1 = \nu_2$  のことと定義する。 $\nu = (n, i)$  を拡張リーフ識別子とし、この識別子で識別される順次集約木リーフがあるとき、該リーフを  $leaf(\nu) = leaf(n, i)$  と表す。 $leaf(\nu)$  を単に、リーフ $\nu$ と呼ぶこともあり、 $leaf(\nu)$  が監査点（あるいはユーザ点）であるときは、監査点 $\nu$ （あるいはユーザ点 $\nu$ ）と呼ぶこともある。

【0114】

また、ある順次集約木SBTのリーフ  $leaf(SBT, i)$  について、この順次集約木SBTのリーフに順次割当値を割り当てる元となった証明要求の受付時刻を、該リーフに対応する時刻といい、これを  $time(SBT, i)$  あるいは簡単に  $time(i)$  と表す。同様に、 $leaf(\nu)$  について、このリーフに順次割当値を割り当てる元となった証明要求の受付時刻を、 $time(\nu)$  と表す。

【0115】

利用者装置2iが、監査装置3を用いて、ある受理証明書に対する第2の検証を実行するには、上述したように該受理証明書に対応する順次集約木リーフ $\tau$ と、該受理証明書に対する遅延補完データ要求に対応する順次集約木リーフ  $\tau'$  の間 ( $\tau$  と  $\tau'$  も含む) に監査装置3の監査点 $\alpha$ が存在する必要がある。このためには、 $T$ をある正整数とし、以下の3つの条件(1)、(2)、(3) が成り立てば十分である。

【0116】

(1) 監査装置3の最初の監査点の時刻は  $T$  より小さい。

【0117】

(2) 監査装置3による任意の1つの監査点を $\alpha$ 、次の監査点を $\alpha'$ とすると、 $time(\alpha') - time(\alpha) \leq T$  が成り立つ。

【0118】

(3) 利用者装置2iは、拡張リーフ識別子 $\tau$ の順次集約木リーフで受理証明書を受信し

た後のある順次集約木リーフ $\tau'$ で該受理証明書に対する遅延補完データを受信することとし、

$\text{time}(\tau') - \text{time}(\tau) \geq T$ が成り立つ。

【0119】

尚、これらの条件の十分性の理由に関しては後述する(後述の次集約木の性質3の(1)と(2)を参照)。

【0120】

図9に示すようなある順次集約木SBTに属する監査装置3の監査点 $\alpha$ において、監査装置3は監査用受理証明書を受信するものとする。監査用受理証明書には、 $\alpha$ における即時補完データが含まれている。この即時補完データには、順次集約木SBTの任意のリーフ $\tau$ で $\alpha$ より左にあるものの割当値 $V(\tau)$ が次のような意味で結合している。即ち、 $\tau$ の $\alpha$ による認証点 $p2$ の割当値 $V(p2)$ が上記の即時補完データに含まれ、この認証点の割当値は $V(\tau)$ から出発して $\text{authPath}(\tau)$ に属する幾つかのノードの割当値をハッシュ関数 $h$ によりリンクすることにより計算できる(これが成立つ理由については、後述の順次集約木の性質2の項目(1)を参照)。

【0121】

これにより、監査装置3は監査点 $\alpha$ で受信した監査用受理証明書内の即時補完データに、上記 $V(p2)$ が含まれているか否かにより、利用者がユーザ点 $\tau$ で取得した受理証明書の元となった要求の送信及び証明装置1による要求受けが、監査装置3が監査点 $\alpha$ で取得した監査用受理証明書の受信より時間的に前であることを検証することができる(これを検証結果1とする。図10を参照)。

ここで、証明装置1の直列化可能性について説明する。証明装置1の直列化可能性とは、該証明装置が任意の複数の順序証明要求を受付け処理する際に、該複数の要求を直列に並べるある順序付けがあり、その順序に従って順次受けて、それに対する処理結果である受理証明書を返信し、その後次の要求の処理を行った場合と同じ結果となることと定義する。

【0122】

証明装置の直列化可能性は重要な要件であり、本実施の形態においては、直列化可能性を保証する手段を有するものとする。このような手段としては、証明装置が1つ順序証明要求を受付けたとき、該要求に対する受理証明を送信してからのみ次の要求受けけることを監視する直列性監査装置を用いてもよい。

【0123】

この直列化可能性を用いれば、ユーザ点と監査点の順序関係について検証結果1より強いことを結論することができる。例えば、順序証明装置1の直列化可能性が、監査装置3が監査点 $\alpha$ で取得した受理証明書の受信時まで保証されていたとすると、上記検証により、ユーザ点 $\tau$ に対応する順序証明要求の受けが、監査点 $\alpha$ に対応する監査用順序証明要求の受けより時間的に前であることを結論できる(これを検証結果2とする。図10を参照)。なぜならば、直列化された順序証明要求の処理において、 $\alpha$ に対応する監査用順序証明要求の受けが $\tau$ に対応する監査用順序証明要求の受けより前であれば、 $\alpha$ に対応する受理証明書 $EOC(\alpha)$ は、 $\tau$ に対応する監査用順序証明要求 $EOR(\tau)$ の受けより前に送信されることになり、 $EOC(\alpha)$ に $EOR(\tau)$ が含むイベント値がハッシュ関数を介して結合するデータを含めることは出来ないからである。以上から、監査装置3が監査点 $\alpha$ で取得した監査用受理証明書の受信時まで、証明装置1の直列化可能性が推認されるときには、ユーザ点 $\tau$ に対応する順序証明要求の受けは、監査点 $\alpha$ に対応する監査用順序証明要求の受けより時間的に前であることが推認される。以後、このことを「ユーザ点の未来側の境界付け」という。

【0124】

尚、監査装置3が監査点 $\alpha$ で取得した監査用受理証明書の受信時までの証明装置1の直列化可能性を保証しても、監査装置3が受理証明の一部として即時補完データを受信していなければ、上記のことは言えないことに注意する必要がある。なぜならば、監査装置3が



監査点 $\alpha$ で取得した監査用受理証明書の受信時より後に、証明装置 $\gamma$ における割当て値を変更する可能性を除外することはできないからである。

#### 【0125】

従って、第1の実施の形態のイベント順序証明システム100によれば、利用者装置2iから証明要求を受付けた証明装置1が、該要求に含まれるデジタル・データから計算される順次割当て値及び前記順次割当てデータが割り当てられた順次集約木の位置情報を含む受理証明書及び補完データを発行し、補完情報順次集約木のルート値に対して高強度デジタル署名を付す等の手段により真正性を保証しながら電子的に公表するので、利用者装置2iは公表情報および補完データから簡単に受理証明書の検証をすることができる。また、順次集約木のルート値を電子的に公表する前であっても、監査装置3が順次集約木の監査点に関する監査情報を有しているので、監査装置5は利用者装置2iからの監査要求を受けて、受理証明書の監査をすることができる。

#### 【0126】

この結果、受理証明書の正当性を検証できたときには、証明装置1における監査対象とした受理証明書の証明要求受信が、監査に用いた監査用受理証明書の証明要求受信よりも時間的に前であることを証明することができる。

#### 【0127】

<第2の実施の形態>

(2-1. システム構成)

図11は、本発明の第2の実施の形態に係るイベント順序証明システム200のシステム構成図である。同図に示すイベント順序証明システム200は、イベント順序証明装置（以下、証明装置という）7、複数のイベント順序証明利用者装置（以下、利用者装置という）2i ( $i=a, b, \dots, n$ )、証明装置7が発行したイベント順序受理証明書（以下、受理証明書という）の監査を行うイベント順序証明監査装置（以下、監査装置という）8、及び、以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成されるコンピュータネットワーク4を備えており、証明装置7が利用者装置2iからのイベント順序証明要求（以下、証明要求という）に応じて、受理証明書を発行し、利用者装置2iに返信すると共に、受理証明書に疑義が生じた場合には、利用者装置2iは、証明装置7が公表したデータ又は監査装置8による監査結果によって受理証明書を検証することができるようになっている。

#### 【0128】

ここで、第2の実施の形態は、第1の実施の形態とほぼ同様のシステム構成であるが、監査装置8が、各順次集約期間の終了後に、その順次集約期間中に取得した各監査用受理証明書の完全遅延補完データを、証明装置7に要求して（あるいは事前の契約に基づいて）取得するという点が異なっている。尚、本実施の形態においては、第1の実施の形態と異なる構成及び機能を説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

#### 【0129】

また、第1の実施の形態と同様に第2の実施形態においても、イベント順序証明システム200のシステム構成は機能が同一であればその形態は問わないものであり、その物理的構成は種々考えられるものである。例えば、利用者装置2iの代わりに、利用者検証装置6iが受理証明書の検証を行うようにしてもよいし、証明装置7の代わりに、電子的情報公表装置5が証明装置7から公表データをもらい、公開するようにしてもよい。また、コンピュータネットワーク4は、郵便など他の通信手段に置き換えることも可能である。

#### 【0130】

証明装置7は、コンピュータネットワーク4を介して利用者装置2i及び監査装置8とデータの送受信を行う送受信部11、利用者装置2iからの証明要求として送信されたデジタル・データを順次集約木を用いてまとめるイベント順序証明要求集約部12、受理証明書を作成するイベント順序証明作成部13、監査装置8に送信する監査情報を作成する監査情報作成部14、利用者装置2iからの補完データ要求に応じて補完データを取得する補完データ取得

部15、証明装置7が一定期間に発行した複数の受理証明書の内容を連結したデータに対して高強度デジタル署名をする高強度デジタル署名作成部16、高強度デジタル署名されたデータを電子的に公表する電子的情報公表部17、及び受理証明書をはじめとするイベント順序証明に関する情報を記憶する記憶部12を有する構成である。

#### 【0131】

監査情報作成部71は、各監査点における監査用受理証明書を順次集約木から取得して作成することに加えて、各順次集約期間の終了後に、その順次集約期間に取得した各監査用受理証明書の完全遅延補完データを取得して作成するようになっている。

#### 【0132】

監査装置8は、コンピュータネットワーク4を介して証明装置7および利用者装置2iとデータを送受信する送受信部31、証明装置7に各監査用受理証明書の完全遅延補完データの要求を行う補完データ要求部81、利用者装置2iからある受理証明書の監査要求を受けた際には、利用者装置2iから送信された監査要求情報及び監査情報（監査用受理証明書に加えて該監査用受理証明書の完全遅延補完データも含める）を用いて受理証明書の検証を行い、その結果を利用者装置2iに返信するイベント順序証明監査部82、及び監査用受理証明書をはじめとする監査情報を記憶する記憶部83を有する構成である。

#### 【0133】

イベント順序証明監査部82は、第1の実施の形態のイベント順序証明監査部32の機能（「ユーザ点の未来側の境界付け」）に加えて、後述する「ユーザ点の過去側の境界付け」を検証できる機能を有するようになっている。これは、あるユーザ点がある監査点よりも左にあること（即ち、時間的に前にあること）に加えて、あるユーザ点がある監査点よりも右にあること（即ち、時間的に後であること）を監査できることを意味する。

#### 【0134】

以下、図12を参照しながら、この「ユーザ点の過去側の境界付け」について説明する。

#### 【0135】

尚、以下では、監査装置8が各順次集約期間の終了後に、その順次集約期間に取得した各監査用受理証明書の完全遅延補完データを取得することを、監査装置8は複合完全補完を行うという。

#### 【0136】

本実施の形態においては、監査装置8は、順次集約期間が終わるごとに、該順次集約期間に受信した監査用受理証明書に対する完全遅延補完データを取得するので、監査用受理証明書に含まれる即時補完データと該遅延補完データを組み合わせることにより、監査装置8は、該順次集約期間に受信した監査用イベント受理証明書に対する完全補完データを取得することになる。

#### 【0137】

ここで、利用者装置2iと監査装置8は、第1の実施の形態で述べた条件（1）（2）及び（3）を満たすものとする。 $\tau$ を利用者装置2iによるユーザ点で、 $T \leq \text{time}(\tau)$ を満たすものとする。 $T \leq \text{time}(\tau)$ という条件から、上述の条件（1）により $\tau$ より左にある（即ち時間的に前にある）監査装置8による監査点が存在する。そのような監査点の一つを $\alpha 1$ とおく。 $\alpha 1$ として、上記条件を満たす監査点のうち最も右に位置するものをとることにしてもよい。監査は以下の手順に従って実行される。

#### 【0138】

（1）利用者装置2iがユーザ点 $\tau$ で取得した受理証明書（順次集約木リーフ番号、即時補完データ）を監査装置8に送付する。

#### 【0139】

（2）監査装置8は利用者装置2iから送付された受理証明書に含まれる順次集約木リーフ番号を取り出し、該受理証明書に対応する順次集約木リーフ $\tau$ を特定し、自分が取得した監査用受理証明書の中から、 $\tau$ より左に位置する順次集約木リーフに対応するものを選ぶ。このような監査用受理証明書の中から、対応する順次集約木リーフがもっとも右に位置

するものを選んでよい。このように選ばれた監査用受理証明書に対応する順次集約木リーフを $\alpha 1$ とする。

#### 【0140】

(3) 監査装置8は複合完全補完を行うので、監査装置8は監査点 $\alpha 1$ に対応する監査用受理証明書の完全遅延補完データを取得する。該遅延補完データに対応する順次集約木リーフは、 $\tau$ と等しいか右に位置する(時間的に後である)。

#### 【0141】

(4) 監査装置8は、監査点 $\alpha 1$ に対応する監査用受理証明書とそれに対する上記遅延補完データから、監査点 $\alpha 1$ のユーザ点 $\tau$ による認証点 $p 2$ の割当値を計算することができる。

#### 【0142】

(5) 従って、監査装置8は、利用者装置2iから受信した順次集約木リーフ $\tau$ に対応する受理証明書内の即時補完データに、上記計算した監査点 $\alpha 1$ のユーザ点 $\tau$ による認証点の割当値が含まれることを検証することにより、 $\alpha 1$ が $\tau$ より左に位置することを監査することができる。

#### 【0143】

この検証結果からまず言えることは、監査点 $\alpha 1$ に対応する監査装置7の監査用証明要求が証明装置7に受信された時刻を $t1$ 、 $\tau$ に対応する利用者装置2iの証明要求が証明装置7に受信された時刻を $t2$ 、この要求に対する受理証明書が証明装置7から送信された時刻を $t2'$ とおくと、 $t1 < t2'$ ということである。

#### 【0144】

ここで、本実施の形態においても、証明装置7の直列化可能性は保証されている、即ち、 $t2'$ の時点まで証明装置7の直列化可能性は保証されているとすると、さらに、 $t1 < t2'$ ということも結論できる。以上から、証明装置7がユーザ点 $\tau$ に対応する受理証明書を利用者装置2iに送信した時刻まで、証明装置7の直列化可能性が推認されるときには、監査点 $\alpha 1$ に対応する監査用証明要求の受付けは、ユーザ点 $\tau$ に対応する利用者装置2iの証明要求の受付けより時間的に前であることが推認される。

#### 【0145】

尚、 $t2'$ 時点までの証明装置7の直列化可能性を保証しても、利用者装置2iが受理証明の一部として即時補完データを受信していなければ、上記のことは言えないことに注意する必要がある。なぜならば、 $t2'$ 時点より後で、証明装置7が監査点 $\alpha 1$ における割当て値を変更する可能性を除くことはできないからである。

#### 【0146】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置(CPU: Central Processing Unit)、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置(メモリ)、ハードディスク(HD)等の電源断時にもデータを記憶し続けることが出来る2次記憶装置を有する電子的な装置から構成されている。このうち、証明装置7の監査情報作成部71、並びに監査装置8の補完データ要求部81及びイベント順序証明監査部82の処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、証明装置7の記憶部72及び監査装置8の記憶部83は、上記主記憶装置あるいは2次記憶装置の機能を備えたものである。

#### 【0147】

また、本実施の形態に係る各種処理を実行するプログラムは、前述した主記憶装置または2次記憶装置に格納されているものである。そして、このプログラムは、ハードディスク、フレキシブルディスク、CD-ROM、MO、DVD-ROMなどのコンピュータ読み取り可能な記録媒体に記録することも、通信ネットワークを介して配信することも可能である。

#### 【0148】

### (2-2. システム動作)

次に、以上の構成を有するイベント順序証明システム200におけるイベント順序証明方

法、およびイベント順序証明検証方法を図13及び図14を用いて説明する。ここで、図13は、1つの順次集約期間において証明装置7がイベント受理証明書及び監査用受理証明書を作成する動作を説明するシーケンス図であり、図14は、利用者装置2iがイベント受理証明書に対して第2の検証を行う動作を説明するシーケンス図である。

#### 【0149】

まず、図13に示すイベント順序証明方法について説明する。尚、本実施の形態に係るイベント順序証明方法において、その動作のほとんどは第1の実施の形態と同様であり、図6のステップS10～S200は、図13のステップS610～S800と同一で、その後のステップS810～S850が新たに追加されたものである。従って、以下ではこの追加されたステップについてのみ説明する。

#### 【0150】

順次集約のための一定期間が終了すると、証明装置7の監査情報作成部71は、監査装置8からの完全遅延補完データ要求に対して、この集約期間内に発行した各監査用受理証明書の完全遅延補完データを取得し、監査装置8に送信する（ステップS810、S820、S830、S840）。

#### 【0151】

これにより、監査装置8は、各監査用受理証明書の完全遅延補完データを受信する（ステップS850）。

尚、図13に示すイベント順序証明方法においては、監査装置8の方から証明装置7に完全遅延補完データ要求を送信し、これに応じて証明装置7が監査装置8に完全遅延補完データを送信する方式であったが、これとは異なり、証明装置7が監査装置8に完全遅延補完データを自動的に送信するような方式であってもよい。

#### 【0152】

次に、図14を参照しながら、監査装置3を用いたイベント順序証明検証方法について説明する。これは、利用者装置2iの第2の検証機能に相当するものである。ここで、利用者装置2iの第2の検証機能に関しては、第1の実施の形態の検証機能（「ユーザ点の未来側の境界付け」）に、新たな検証機能（「ユーザ点の過去側の境界付け」）が加わったものであり、この新たな機能の動作を示すのが図14である。即ち、本実施の形態の「ユーザ点の未来側の境界付け」に関する検証処理は、第1の実施の形態で示された図8の動作と全く同一であるため、説明は省略し、「ユーザ点の過去側の境界付け」に関する検証処理について説明する。また、利用者装置2iの第1の検証機能に相当する検証方法については、第1の実施の形態における検証方法と同一であるため、説明を省略する。

#### 【0153】

まず、利用者装置2iは、監査の対象となる受理証明書（但し、即時補完データは含まれている）を含む監査要求情報を監査装置8に送信する（ステップS910、S920）。

#### 【0154】

次に、監査装置8は送受信部31を介して監査要求情報を受信すると、イベント順序証明監査部82は、利用者装置2iから送信された監査要求情報に含まれる受理証明書が割り当てられた順次集約木のリーフを特定し、該リーフより左に位置する監査点 $\alpha 1$ を計算する（ステップS930、S940）。そして、この監査点 $\alpha 1$ の監査用受理証明書および該監査用受理証明書の完全遅延補完データを取得する（ステップS950）。

#### 【0155】

続いて監査点 $\alpha 1$ のリーフによる認証点を計算し、監査点 $\alpha 1$ の監査用受理証明書および該監査用受理証明書の完全遅延補完データから認証点の割当値 $A_{ca1}$ を計算する（ステップS960、S970）。一方、イベント順序証明監査部82は、監査要求情報として既に受け取っている受理証明書の即時補完データからこの認証点の割当値 $A$ を取得して、この認証点の割当値 $A$ が、計算により求めた認証点の割当値 $A_{ca1}$ に一致するか否かを検証する（ステップS980、S990）。

#### 【0156】

以上の検証において、検証に成功すれば、受理証明書が改ざんされていないことを確認

することができる（ステップS995）。一方、検証に失敗すれば、受理証明書が改ざんされていることを確認することができる（ステップS1000）。そして、イベント順序証明監査部82は、この監査結果を送受部31を介して利用者装置2iに送信し、利用者装置2iは、監査結果を受信する（ステップS1010、S1020）。

#### 【0157】

これにより、利用者装置2iは、電子的公表機関を介した公表前においても、証明装置7が発行した受理証明書が当該の順次集約期間において、受理証明書に含まれる元デジタル・データに対して、受理証明書に含まれる順次集約木リーフ番号で識別される順番において発行されたものであることを確実に検証することができるとともに、ユーザ点の過去側の境界付けを検証することができる。尚、上記監査結果に監査点 $\alpha$ 1の識別子を含めてもよい。この場合においては、利用者装置2iは、上記監査を要求した受理証明書に対応する証明要求の登録が、監査点 $\alpha$ 1に対応する監査用証明要求の登録より後であったことの保証を監査装置8から確実に得ることができる。

#### 【0158】

尚、以上においては、「ユーザ点の過去側の境界付け」に関する検証処理の動作を説明したが、監査装置8は、「ユーザ点の未来側の境界付け」とともに「ユーザ点の過去側の境界付け」に関する検証処理を行うようにしてもよく、この場合には、監査要求情報として、第1の実施の形態における受理証明書および遅延補完データが必要となる。

#### 【0159】

従って、第2の実施の形態のイベント順序証明システム200によれば、第1の実施の形態と同じ効果を得ることができる。また、これに加えて、受理証明書の正当性を検証できたときには、証明装置7において監査対象とした受理証明書の証明要求受信が監査に用いた監査用受理証明書の証明要求受信よりも時間的に後であることを証明することができる。

以上、第2の実施の形態について説明したが、第2の実施の形態には種々の変形例が考えられるものである。以下、第2の実施の形態の変形例について説明する。

#### 【0160】

（2-3. 第2の実施の形態の変形例1）

監査装置8は、上述した「ユーザ点の未来側の境界付け」及び「ユーザ点の過去側の境界付け」の機能から、2つのユーザ点の間の順序の判定を示すことも可能である。次に、2つの利用者装置2aと2bが各々、順次集約木リーフ $\tau$ と $\tau$ 1において受理証明書を取得するとき、監査装置8が $\tau$ と $\tau$ 1の前後関係を監査する方法について図15を参照して説明する。ここで、図15は、監査装置8が $\tau$ と $\tau$ 1の前後関係を監査する動作を示すフローチャート図である。

#### 【0161】

以下、順次集約木のリーフ $\tau$ 、 $\tau$ 1について、 $\tau$ （或いは $\tau$ 1）の時点とは $\tau$ （或いは $\tau$ 1）に割り付けられた順序証明要求を受信した時点を表し、 $\tau \leq \tau$ 1と書くことにより、 $\tau$ の時点以降に $\tau$ 1の時点があることを表す。以下では、 $\tau$ と $\tau$ 1の大きい方を $\tau$ 2とし、 $\tau$ 2で受信した順序証明要求に対する受理証明の送信の時点までは証明装置1の直列化可能性が保証されているものとする。

#### 【0162】

尚、利用者装置2a及び2bと監査装置8は、それぞれ第1の実施の形態の「ユーザ点の未来側の境界付け」の説明で述べた条件（1）（2）及び（3）を満たすものとする。

#### 【0163】

まず、監査装置8が、利用者装置2a及び2bより、各受理証明書のユーザ点間の順序判定要求を受けると、 $\tau$ に等しいか右に位置する監査装置8の監査点で最も左に位置するものを $\alpha$ とし、 $\tau$ 1に等しいか右に位置する監査装置8の監査点で最も左に位置するものを $\alpha$ 1として、決定する（ステップS1110、S1120、S1130）。

#### 【0164】

次に、監査点 $\alpha$ と $\alpha$ 1の時間的前後を比較する（ステップS1140）。これは、各監査点

の監査用受理証明書の順次集約木番号及び順次集約木リーフ番号から判断するものである。

【0165】

$\alpha < \alpha_1$  のときは、第1の実施の形態の「ユーザ点の未来側の境界付け」及び上記「ユーザ点の過去側の境界付け」で述べた方法により、以下のように  $\tau < \tau_1$  が示される（ステップS1150）。

【0166】

これは、 $\tau_1$  に等しいか左に位置する監査装置8の監査点でもっとも右に位置するものを  $\alpha_2$  とおくと、 $\alpha \leq \alpha_2$  であり、また、「ユーザ点の未来側の境界付け」で述べた方法により、 $\tau \leq \alpha$  が示されるとともに、「ユーザ点の過去側の境界付け」で述べた方法により、 $\alpha_2 \leq \tau_1$  が示されるので、以上より、 $\tau < \alpha \leq \alpha_2 < \tau_1$  となり、 $\tau < \tau_1$  が導かれるものである。

【0167】

同様に、 $\alpha_1 < \alpha$  のときは、 $\tau_1 < \tau$  が示される（ステップS1180）。

$\alpha = \alpha_1$  のときは、 $\tau$  と  $\tau_1$  の前後関係の判定は、以下の手順（1）～（4）に従って行われる。

【0168】

（1）利用者装置2aが  $\tau$  とその遅延補完点  $\tau'$  で取得する情報からユーザ点  $\tau$  の監査点  $\alpha$  による認証点の位置と割当値が計算され、監査装置8が監査点  $\alpha$  で取得する監査用受理証明書に含まれる即時補完データに上記認証点の割当値が含まれていることにより、監査装置8は  $\tau$  が、 $\alpha$  より左にあること、さらに  $\tau$  が、 $\alpha$  より、幾つ左にあるかを判定する。ここで、 $\tau$  が、 $\alpha$  より  $n$  個左にあるものとする（ステップS1160）。

【0169】

（2）同様に、利用者装置2bが  $\tau_1$  とその遅延補完点  $\tau'_1$  で取得する情報から  $\tau_1$  の監査点  $\alpha$  による認証点の位置と割当値が計算され、監査装置8が監査点  $\alpha$  で取得する監査用受理証明書に含まれる即時補完データに上記認証点の割当値が含まれていることにより、監査装置8は  $\tau_1$  が、 $\alpha$  より左にあること、さらに  $\tau_1$  が、 $\alpha$  より、幾つ左にあるかを判定する。ここで、 $\tau_1$  が、 $\alpha$  より  $n_1$  個左にあるものとする（ステップS1160）。

【0170】

（3） $n > n_1$  のときは、監査装置8は、利用者装置2aによるユーザ点  $\tau$  が利用者装置2bによるユーザ点  $\tau_1$  より左に位置することを示すことができる（ステップS1170）。また、 $n < n_1$  のときは、監査装置8は、利用者装置2aによるユーザ点  $\tau$  が利用者装置2bによるユーザ点  $\tau_1$  より右に位置することを示すことができる（ステップS1170）。

【0171】

従って、第2の実施の形態の変形例1によれば、第2の実施の形態の効果に加えて、複数の受理証明書の時間的順序の判定をすることができる。

【0172】

（2-4. 第2の実施の形態の変形例2）

また、監査装置8は、各順次集約期間の終了後に、その順次集約期間に取得した各監査用受理証明書の完全遅延補完データを取得する（複合完全補完を行う）と同時に、各監査用受理証明とその完全補完データから順次集約木のルート値を計算し、計算されたルート値が公表されたルート値に一致するか否かを検証することが可能である。このことを監査装置8による「複合完全化によるルート値検証」と呼ぶ。

【0173】

これは、図16に示すように、監査装置8が、順次集約木のルート値を計算し、計算したルート値が、証明装置7から公表されたルート値と一致するか否かを検証することで、証明装置7による不正が行われていないことを検証するものである（ステップS1210、S1220、S1230、S1240、S1250）。

【0174】

また、監査装置8は、この「複合完全化によるルート値検証」の機能により、利用者装

置2iからの監査要求に含まれる監査要求情報の正当性を検証することができる。

【0175】

例えば、ある順次集約木SBTの構成終了後に、利用者装置2aが、リーフ(0,  $\tau$ )の割当値を本来の割当値 $V(\tau)$ から割当値 $v'$ に改変し、割当値 $v'$ が $V(\text{root}(\text{SBT}))$ にハッシュ関数 $h$ によりリンクすることを主張したとする。このとき、第三者にこの主張を認めさせるためには、利用者装置2aは、リーフ(0,  $\tau$ )の補完データ

$[(v(0), LR(0)), (v(1), LR(1)), \dots, (v(k-1), LR(k-1))]$

を用意し、 $v'$ とこの補完データをハッシュ関数 $h$ により所定の方式で組み合わせることにより $V(\text{root}(\text{SBT}))$ が計算できることを示さなければならない。この計算の過程においては、ユーザ点 $\tau$ の監査点 $\alpha$ による認証点(図9のp2)の割当値 $v2'$ も計算される。 $v2'$ はハッシュ関数の衝突困難性によって(実用上無視できる確率を除いて) $\text{round}(\alpha)$ において監査装置8に送付されたp2の割当値 $V(p2)$ とは異なる。一方、監査装置8は、 $V(\alpha)$ から出発し、 $\text{authPath}(\alpha)$ に属するノードの割当値をハッシュ関数 $h$ によりリンクすることにより $V(\text{root}(\text{SBT}))$ を計算する。p2は $\text{authPath}(\alpha)$ に属するので、 $V(p2)$ も結合される値の1つである。ここで(実用上無視できる確率を除いて) $v2' \neq V(p2)$ であるから、再びハッシュ関数の衝突困難性により、利用者装置2aが計算によって示す $\text{root}(\text{SBT})$ の割当値と監査装置8が複合完全化によるルート値検証において計算する $\text{root}(\text{SBT})$ の割当値とは(実用上無視できる確率を除いて)異なることになる(この点についての詳細は、後述の順次集約木の性質4を参照)。従って監査装置8は利用者装置2aの主張が誤りであることを検出することができる。

【0176】

従って、第2の実施の形態の変形例2によれば、第2の実施の形態の効果に加えて、電子的情報公表機関が公表した順次集約木のルート値の正当性を検証することができる。また、監査装置8のルート値検証機能により、証明装置1及び利用者装置2iのいずれかにおいて不正があったとしても、不正の切り分けをすることができる。

【0177】

(2-5. 第2の実施の形態の変形例3)

また、監査装置8は、利用者装置2iに完全補完データを提供する機能を備えることができる。以下、このことを補完データ完全化という。これは、証明装置1が障害などでサービス中断したときに有効に機能するものである。また、証明装置1がサービス中断しなくても、公表データ公開時や、補完データ要求が一時に大量に発生したときなどに証明装置1の負荷軽減に役立つものである。

【0178】

図17を参照して補完データ完全化について説明する。

【0179】

図17において、監査装置8が監査点aの完全補完データを持つならば、該完全補完データと利用者装置2iが、イベント受理証明書を取得するユーザ点uとその遅延補完データを取得する点u'で取得する情報を組み合わせることによりユーザ点uの完全補完データを計算することができる(以下、性質P1という)。

【0180】

なぜならば、図17で、j1はユーザ点uの監査点aによる認証点のレベルであり、ユーザ点uの認証パス情報のうち、レベルj1より小さいノードの情報はユーザ甲が取得しており、レベルj1以上kより小さいノードの情報は監査装置8が取得しているからである。但し、kは順次集約木の高さである。

【0181】

例えば、公開間隔が1週間とし、1日級の監査装置8(少なくとも1日に一回監査情報を取得し、各監査点の完全補完データを取得する機関)があるものとする。利用者装置2iは受理証明書を取得したのち、1日以上経過してから、遅延補完データを取得することにより、利用者装置2iの取得する情報と、監査装置8の取得する情報を組み合わせることにより利用者装置2iが取得した受理証明書の完全補完データを構成することができる(上記性質

Plによる)。

#### 【0182】

次に図18を参照して、2つ以上の監査装置8i (i=a, b, n) を介して利用者装置2iが完全補完データを取得する方法について説明する。尚、監査装置8iとしては、上述した1日級の監査装置8a (少なくとも1日に一回監査情報を取得し、各監査点の完全補完データを取得する機関) と監査装置8a依存の1時間級の監査装置8b (少なくとも1時間に一回監査情報を取得し、各監査点の遅延補完データ点を監査装置8aの監査点を挟むように設定する装置) があるとする。

#### 【0183】

このとき利用者装置2iは受理証明書を所得したのち、1時間以上経過してから、遅延補完データを取得することにより、利用者装置2iの取得する情報、監査装置8bの取得する情報、及び監査装置8aの取得する情報を組み合わせることによりユーザ点の完全補完データを構成することができる。

#### 【0184】

このことは、上記性質Plを繰り返し用いることにより示される。まず、監査装置8aの取得する情報と監査装置8bの取得する情報を組み合わせることにより、監査点a2の認証パス情報が得られる。従って、図17の場合の例と同様に、ユーザ点Uの認証パス情報が得られる。

#### 【0185】

尚、上述した監査装置8a及び8bの監査点に関する条件は、例えば、監査装置8a依存の1時間級の監査装置8bは、自己の各監査点の遅延補完データを1日以上たってから取得してもよいし、あるいは1日級の監査装置8aの監査点が1日の定時 (例えば午前0時) に取得されることが分かっているならば、毎日の監査点の遅延補完データを、その日の終了後にまとめてとるようにしてもよい。また、上記例においては2つのレベルの監査装置8iを利用してはいるが、同様に3つ以上のレベルの監査装置8iを利用することも可能である。

#### 【0186】

##### <第3の実施の形態>

##### (3-1. システム構成)

図19は、本発明の第3の実施の形態に係るイベント順序証明システム300のシステム構成図である。同図に示すイベント順序証明システム300は、イベント順序証明装置 (以下、証明装置という) 1、時刻情報提供装置30、複数の時刻証明利用者装置 (以下、利用者装置という) 10j (j=a, b, ..., n)、複数のイベント順序証明利用者装置&時刻証明装置 (以下、利用者装置 (時刻証明装置) という) 20i (i=a, b, ..., n)、イベント順序証明監査装置&イベント時刻監査装置 (以下、監査装置という) 9、及び、以上の各装置を相互に接続する、例えば、インターネット網、電話回線網などにより構成されるコンピュータネットワーク4を備えており、イベント順序証明を行うとともに、時刻証明を行うコンピュータシステムとなっている。即ち、利用者装置 (時刻証明装置) 20iは、上記実施の形態の利用者装置2iの機能に加えて、時刻証明を行う時刻証明装置の機能も備えており、利用者装置10jからの時刻証明要求に応じて、時刻受理証明書を発行し、利用者装置10jに返信するようになっている。また、利用者装置20iが、上記時刻受理証明書のダイジェストを含むイベント順序証明要求 (以下、証明要求という) を証明装置1に送信すると、証明装置1は、該証明要求に応じて、イベント順序受理証明書 (以下、受理証明書という) を発行し、利用者装置20iに返信するようになっている。そして、この受理証明書に疑義が生じた場合には、利用者装置20iは、証明装置1が公表したデータ又は監査装置9による監査結果によって受理証明書を検証できるとともに、受理証明書と時刻受理証明書が対応付けられているので、区間時刻証を取得できるようになっている。

#### 【0187】

尚、本実施の形態においては、上記実施の形態と異なる構成及び機能を説明し、その他の構成及び機能に関しては同一部分には同一符号を付して説明を省略する。

#### 【0188】



また、上記実施の形態と同様に、第3の実施形態においても、イベント順序証明システム300のシステム構成は機能が同一であればその形態は問わないものであり、その物理的構成は種々考えられるものである。例えば、利用者装置（時刻証明装置）20iの代わりに、利用者検証装置（時刻証明装置）60iが受理証明書の検証を行うようにしてもよいし、証明装置1の代わりに、電子的情報公表装置5が証明装置1から公表データをもらい、公開するようにしてもよい。また、コンピュータネットワーク4は、郵便など他の通信手段に置き換えることも可能である。

#### 【0189】

さらに、本実施の形態においても、第1の実施の形態と同様に証明装置1の直列化可能性は保証されているものとする。保証の手段としては、第1の実施の形態におけると同様、直列化可能性監査装置を用いることにしてもよい。

#### 【0190】

時刻情報提供装置30は、正確な時刻情報を保持して、利用者装置（時刻証明装置）20i及び監査装置9に時刻情報を提供するようにになっている。

#### 【0191】

利用者装置10jは、利用者装置（時刻証明装置）20iに所定のデジタル・データを含む時刻証明要求をし、その応答として利用者装置（時刻証明装置）20iから時刻情報が付された時刻受理証明書を取得するようにになっている。

#### 【0192】

利用者装置（時刻証明装置）20iは、上述したように利用者装置2iの機能に時刻証明装置の機能を付加した装置で、コンピュータネットワーク4を介して証明装置1、監査装置9、利用者装置10j及び時刻情報提供装置30とデータを送受信する送受信部21、利用者装置10jからの時刻証明要求を受け付けて時刻受理証明書を作成する時刻証明作成部201、時刻受理証明書ダイジェストを含む証明要求を行うイベント順序証明要求部202、現時点において取得可能な受理証明書に対する補完データを要求する補完データ要求部23、受理証明書を検証するイベント順序証明検証部204、受理証明書をはじめとするイベント順序証明に関する情報及び時刻受理証明書をはじめとする時刻証明に関する情報を記憶する記憶部205を有する構成である。尚、本実施の形態においては、イベント順序証明利用者装置として、時刻証明装置を兼ねた利用者装置を採用しているが、時刻証明装置を兼ねない利用者装置が存在してもよく、利用者装置（時刻証明装置）20iと利用者装置2iが混在するようなシステム構成としてもよい。

#### 【0193】

詳しくは、時刻証明作成部202は、利用者装置10jから送信された所定のデジタル・データを含む時刻証明要求を受け付けて、該デジタル・データに時刻情報提供装置30から取得した時刻情報を付した時刻受理証明書を作成するようにになっている。

#### 【0194】

イベント順序証明要求部203は、利用者装置10jからの時刻証明要求に対して作成された時刻受理証明書のハッシュ値である時刻受理証明書ダイジェスト（利用者装置（時刻証明装置）20iが予め用意した衝突困難一方向ハッシュ関数を時刻受理証明書に適用した結果）をイベント受理証明要求に含めるようになっている。従って、利用者装置（時刻証明装置）20iが、証明装置1から受信する受理証明書は、その構成において図4に示す通りであるが、元デジタル・データyは、上述したように、時刻受理証明書ダイジェストを含むものとなっている。

#### 【0195】

監査装置9は、第1の実施の形態の監査装置3の機能に加えて、時刻監査装置としての機能を備えており、詳しくは、コンピュータネットワーク4を介して証明装置1、利用者装置（時刻証明装置）20i及び時刻情報提供装置30とデータを送受信する送受信部31、利用者装置20iからある受理証明書の監査要求を受けた際には、利用者装置20iから送信された監査要求情報および監査情報を用いて受理証明書の検証を行い、その監査結果を利用者装置20iに返信するイベント順序証明監査部32、及び検証した受理証明書に対応する時刻受理

証明書に付された時刻の含まれる時間区間を証明する区間時刻証明証を作成する区間時刻証明証作成部91、監査用受理証明書、区間時刻証明証をはじめとする監査情報を記憶する記憶部92を有する構成である。尚、本実施の形態においては、イベント順序証明監査装置としては、イベント時刻監査装置を兼ねた監査装置を採用しているが、イベント時刻監査装置を兼ねない監査装置が存在してもよく、監査装置9と監査装置3が混在するようなシステム構成としてもよい。

#### 【0196】

区間時刻証明証作成部91は、監査用受理証明書を証明装置1から受信したときの時刻を、時刻情報提供装置30から取得して、区間時刻証明証に付すようになっている。従って、区間時刻証明証作成部91で作成される区間時刻証明証には、本実施の形態においては、未来側の境界の時刻印が付されている。これは、第1の実施の形態で述べたように、監査装置3を用いたイベント順序証明検証（利用者装置2iの第2の検証）により、イベント受理証明要求が割り当てられた順次集約木のリーフが監査点のリーフよりも時間的に前であることが証明できるので、イベント順序証明要求の元となる利用者装置10iからの時刻証明要求の受付が、監査装置9が監査用受理証明書を受信した時刻よりも時間的に前であることを証明するものである。ここで、本実施の形態におけるこの区間時刻証明証を「第1種の区間時刻証明証」という。

#### 【0197】

尚、以上の各装置は、少なくとも演算機能及び制御機能を備えた中央処理装置（CPU：Central Processing Unit）、プログラムやデータを収納する機能を有するRAM(Random Access Memory)等からなる主記憶装置（メモリ）、ハードディスク（HD）等の電源断時にもデータを記憶し続けることが出来る2次記憶装置を有する電子的な装置から構成されている。このうち、利用者装置（時刻証明装置）20iの時刻証明作成部202、イベント順序証明要求部203、補完データ要求部204及びイベント順序証明検証部205、並びに監査装置9の区間時刻証明証作成部91の処理は、上記CPUによる演算制御機能を具体的に示したものに他ならない。また、利用者装置（時刻証明装置）20iの記憶部206及び監査装置9の記憶部92は、上記主記憶装置あるいは2次記憶装置の機能を備えたものである。

#### 【0198】

また、本実施の形態に係る各種処理を実行するプログラムは、前述した主記憶装置または2次記憶装置に格納されているものである。そして、このプログラムは、ハードディスク、フレキシブルディスク、CD-ROM、MO、DVD-ROMなどのコンピュータ読み取り可能な記録媒体に記録することも、通信ネットワークを介して配信することも可能である。

#### 【0199】

##### （3-2. システム動作）

次に、以上の構成を有するイベント順序証明システム300におけるイベント順序証明方法およびイベント順序証明検証方法を図20乃至23を用いて説明する。

#### 【0200】

尚、イベント順序証明方法においては、利用者装置（時刻証明装置）20iを利用者装置2i、監査装置9を監査装置3とすれば、全体的な動作は、図6に示す動作とほぼ同一であるため、異なる動作となる利用者装置（時刻証明装置）20iと利用者装置10i間のやりとりを中心に説明する。ここで、図20及び図21は、図6のステップS10に相当するイベント順序証明要求を送信するステップS10'を詳しく説明するシーケンス図である（図20においては、図6のステップS60に相当する受理証明書を受信するステップS60'も含む）。また、図22は、図6のステップS120に相当する監査用受理証明書を受信するステップS120'を詳しく説明するシーケンス図である。

#### 【0201】

また、イベント順序証明検証方法の第1の検証においては、利用者装置20iを利用者装置2iとすれば、図7に示す動作と同一であるため、説明を省略する。また、イベント順序証明検証方法の第2の検証においては、監査装置9を監査装置3とすれば、図8に示す動作

とはほぼ同一であるため、異なる動作となる監査装置9の区間時刻証の作成について説明する。ここで、図23は、図8のステップS520に相当するイベント受理証明書の検証に成功したときのステップS520'を詳しく説明するシーケンス図である。

#### 【0202】

まず、図20を参照して、イベント順序証明方法のイベント順序証明要求を送信するステップS10'について説明する。

#### 【0203】

利用者装置10jが利用者装置（時刻証明装置）20iにデジタル・データを含む時刻証明要求を送信すると、利用者装置（時刻証明装置）20iは送受信部201を介して、該デジタル・データを含む時刻証明要求を受信する（ステップS11'、S12'）。次に、利用者装置（時刻証明装置）20の時刻証明作成部201は、時刻証明要求を受信した時刻を時刻情報提供装置30から取得し、デジタル・データに該時刻を付した時刻受理証明書を作成し、利用者装置10jに送信する（ステップS13'、S14、S15'）。これにより、利用者装置10jは、時刻受理証明書を受信するので、時刻受理証明書を取得することができる（ステップS16'）。

#### 【0204】

次いで、利用者装置（時刻証明装置）20iのイベント順序証明要求部203は、時刻受理証明書のダイジェストを生成し、時刻受理証明書ダイジェストを含む証明要求を作成し、証明装置1に送信する（ステップS17'、S18）。この結果、証明装置1は、送受信部11を介して、証明要求を受信する（ステップS20'）。

#### 【0205】

尚、上述した方法においては、利用者装置10jに時刻受理証明書だけを返信したが、図21に示すように、利用者装置10jに時刻受理証明書に加えて、受理証明書を返信する方法も考えられる。

#### 【0206】

図21においては、ステップS10'のイベント順序証明要求ステップでは、時刻受理証明書を返信せずに、図6のステップS60に相当するステップS60'のイベント受理証明書受信ステップで、時刻受理証明書および受理証明書を返信する。即ち、利用者装置（時刻証明装置）20iは、証明装置1から受理証明書を受信すると、受理証明書および該受理証明書に対応する時刻受理証明書を利用者装置10jに送信するものである（ステップS61'、ステップS62'）。これにより、利用者装置10jは、受理証明書および時刻受理証明書の双方を受信する（ステップS63'）。

#### 【0207】

次に、図22を参照して、監査用受理証明書を受信するステップS120'について説明する。

#### 【0208】

監査装置9は、送受信部31を介して証明装置1から監査用受理証明書を受信すると、監査用受理証明書を受信した時刻を時刻情報提供装置30から取得して、監査用受理証明書と対応付けて記憶部93に記憶する（ステップS121'、S122'、S123'）。

#### 【0209】

次に、図23を参照して、監査装置9によるイベント受理証明書の検証に成功したときのステップS520'について説明する。

#### 【0210】

監査装置9のイベント順序証明監査部32が、利用者装置（時刻証明装置）20iからの監査要求に応じて受理証明書の監査を行い、監査結果がOKであるときには、さらに、監査用受理証明書に付された時刻から、第1種の区間時刻証明証を発行し、該区間時刻証明証を監査結果に含める（ステップS511'、S512'、S513'）。

#### 【0211】

従って、第3の実施の形態のイベント順序証明システム300によれば、第1の実施の形態と同じ効果を得ることができる。また、これに加えて、第1種の区間時刻証明証の発行

により、未来側の境界の時刻印を与えることができる。

#### 【0212】

(3-3. 第3の実施の形態の変形例)

第3の実施の形態においては、第1の実施の形態の監査装置3に時刻監査装置としての機能を備えた監査装置9を用いたが、第2の実施の形態の監査装置8に時刻監査装置としての機能を備えた監査装置9'を用いて第3の実施の形態の変形例としてもよい。

#### 【0213】

この第3の実施の形態の変形例においては、区間時刻証明証作成部91'は、監査用証明要求を証明装置7に送信したときの時刻を、時刻情報提供装置30から取得して、区間時刻証明証に付すようになっている。従って、第3の実施の形態の変形例においては、区間時刻証明証作成部91'で作成される区間時刻証明証には、過去側の境界の時刻印が付されている。

#### 【0214】

これは、第2の実施の形態で述べたように、監査装置8を用いたイベント順序証明検証(利用者装置2iの第2の検証)により、イベント順序証明要求が割り当てられた順次集約木のリーフがある監査点のリーフよりも時間的に後であることが証明できるので、イベント順序証明要求の元となる利用者装置10jからの時刻証明要求に対する利用者装置(時刻証明装置)20iによる時刻受理証明書の送信が、監査装置9'による監査用イベント順序証明要求の送信よりも時間的に後であることを証明するものである。ここで、この区間時刻証明証を「第2種の区間時刻証明証」という。

#### 【0215】

また、第3の実施の形態の変形例においては、監査装置9'は、「第1種の区間時刻証明証」を発行する機能も当然に有するので、未来および過去側の境界の時刻印が付された区間時刻証明証である「第3の区間時刻証明証」を発行することが可能である。これは、イベント順序証明要求の元となる利用者装置10jからの時刻証明要求の受付が、監査装置9が監査用受理証明書を受信した時刻よりも時間的に前であることを証明するとともに、イベント順序証明要求の元となる利用者装置10iからの時刻証明要求に対する利用者装置(時刻証明装置)20iによる時刻受理証明書の送信が、監査装置9'による監査用イベント順序証明要求の送信よりも時間的に後であることを証明するものである。

#### 【0216】

さらに、第3の実施の形態の変形例として、イベント順序証明システム300'は、利用者装置(時刻証明装置)20iの発行する時刻受理証明書と、該時刻受理証明書に付された時刻の時間的前、後、あるいは両方の境界を証明する1つ又は複数の区間時刻証明証を取得し、それに基づき時刻受理証明書に付された時刻の正当性を判定するイベント時刻検証装置(図19に図示せず)を有するシステム構成としてもよい。この場合においては、イベント時刻検証装置は、時刻受理証明書に付された時刻が、上記区間時刻証明証が証明する時間区間の中に、前もって定められた所定の誤差を許して含まれる割合が、前以て定められた所定の値より大きいことに基づき、時刻証明受理証明書に付された時刻の正当性を判定するようになっている。

#### 【0217】

以上、本実施の形態について説明してきたが、本発明の要旨を逸脱しない範囲において、本発明の実施の形態に対して種々の変形や変更を施すことができる。例えば、上記実施の形態においては、順次集約木として二分木を用いたが、本発明は二分木に限定されるものではなく、1つの親が複数の子を持つ有向木であればよいものである。

#### 【0218】

また、上記実施の形態において証明装置1及び7の電子的情報公表部17については特に詳しく述べなかったが、好適には、電子化社会における情報公表は以下のような要件を満たすことが求められる。

#### 【0219】

(1) 複数の独立なエンティティが同一の情報を公表する。

【0220】

(2) 上記複数のエンティティの各々に誰でもがいつでもアクセスできる。

【0221】

(3) 上記複数のエンティティの各々が公表する情報を取得する際に、情報提供元のエンティティ認証が提供され、かつ提供される情報の完全性が保証される。

【0222】

上記の要件のうち、要件(1)については、複数のサービス機関が、ある範囲の情報について業務として提供することにより実現できる。上記実施の形態においては、証明装置と複数の監査装置が順次集約木のルート値等について業務として情報提供を行うことにより、この要件を満足するようにしている。

【0223】

要件(2)については、現在よく普及しているWWWにより情報提供することにより実現できる。

【0224】

要件(3)については、提供する情報に対して公開鍵暗号方式に基づくデジタル署名を付することにより実現できる。この際、デジタル署名の強度が十分強いこと、及びデジタル署名に用いた署名用秘密鍵及びとそれとペアになる公開鍵のその時点での有効性が、公開鍵証明書、CRL(Certificate Revocation List)、OCSPサービス(Online Certificate Status Protocol)等を用いて公開鍵基盤(PKI: Public-Key Infrastructure)により保証されていることが必要となる。上記の鍵ペアのは、情報の要求者が情報を取得する時点で有効であれば十分であり、随時、鍵ペアを更新し、鍵ペアの有効性を保持しつづけることが可能となる。その際、あるキー・ペア $KP1 = (SK1, PK1)$ を新しいキー・ペア $KP2 = (SK2, PK2)$ に置き換える際に、 $KP1$ が有効である間に $KP2$ の署名用秘密鍵 $SK2$ によるデジタル署名を生成することは必ずしも必要ではなく、利用者がアクセスした際に、その時点で有効なキー・ペアを用いてデジタル署名を生成することが要件となる。

【0225】

従来、情報公表手段として新聞等のマスメディアに情報を公表することが行われてきたが、この方法は例えば10年後に特定のマスメディアに公表された情報にアクセスするのが容易ではないことから上記の要件(2)を満たすのが困難であること、さらにアクセスできたとしても上記の要件(3)を満たす形で情報を取得するのが困難であること等の理由で、電子化社会における情報公表の手段として必ずしも適当ではない。

【0226】

<順次集約木の構成および性質>

上記実施の各形態において用いられた順次集約木の動的な構成方法、および性質について説明するが、その前提としてまず、順次集約木の構成に必要な基本関数について説明する。

【0227】

(基本関数)

高さ $k$ の順次集約木は、レベル0からレベル $k$ までのノードで構成されるが、レベル $j$  ( $j=0, 1, \dots, k$ )のノードの数は、 $2^{(k-j)}$ であるので、レベル $j$ 、番号 $i$ のノードを( $j, i$ )と表すことにすると、 $i=0, 1, \dots, 2^{(k-j)} - 1$ となる。

【0228】

以下、実数 $x$ に対して、 $\text{ceiling}(x)$ を $x$ 以上の最小の整数、 $\text{floor}(x)$ を $x$ 以下の最大の整数として、説明する。

【0229】

ノード( $j, i$ ) (但し、 $j < k$ )の親は、( $j+1, \text{floor}(i/2)$ )であるので、

$$\text{parent}(j, i) = (j+1, \text{floor}(i/2))$$

と定義する。また、ノード( $j, i$ ) (但し、 $0 < j$ )の左側の子供は( $j-1, 2 \cdot i$ )、右側の子供は( $j-1, 2 \cdot i + 1$ )であるので、

$$\text{leftChild}(j, i) = (j-1, 2 \cdot i)$$

$$\text{rightChild}(j, i) = (j+1, 2 \cdot i + 1)$$

と定義する。このとき、高さ  $k$  の順次集約木のノード  $(j, i)$  ( $0 \leq i < 2^{(k-j)}$ ) のルート・パス  $\text{rtPath}_k(j, i)$  (ノード  $(j, i)$  からルートに至るノードの列をいう) は、

$$\text{rtPath}_k(j, i) = [(j, r(j)), \dots, (k, r(k))]$$

と表すことができる。但し、 $r(j) = i$ ,  $r(j'+1) = \text{floor}(r(j')/2)$  ( $j' < k$  とし、 $r(j')$  は既に定まっているものとする) であるとする。尚、 $(k, r(k))$  は、順次集約木のルートを表し、常に  $r(k) = 0$  となる。

#### 【0230】

$V(j, i)$  はノード  $(j, i)$  の割当値である。 $V(0, i)$  を  $V(i)$  と書く。 $L$  を  $L \leq k$  なる非負整数、SBT をある順次集約木とすると、SBT の部分グラフ  $B$  がレベル  $L$  の部分木であるとは、SBT に属するレベル  $L$  のあるノード  $p$  があり、 $B$  が  $p$  及び  $p$  の子孫からなる SBT の部分グラフとなっていることと定義する。

#### 【0231】

$B$  が SBT の部分木であるとき、 $\text{leaves}(B)$  は  $B$  のリーフの集合を表すものとする。また  $X$  を SBT のリーフからなる空でない集合とすると、 $\text{first}(X)$  により  $X$  のうち最も左に位置するリーフを表し、 $\text{last}(X)$  により  $X$  のうち最も右に位置するリーフを表す。

#### 【0232】

2つの整数  $i_1, i_2$  について、 $[i_1..i_2]$  は  $i_1 \leq i \leq i_2$  なる整数  $i$  からなる集合 (区間) を表し、 $(i_1..i_2]$  は  $i_1 < i \leq i_2$  なる整数  $i$  からなる集合 (区間) を表し、 $[i_1..i_2)$  は  $i_1 \leq i < i_2$  なる整数  $i$  からなる集合 (区間) を表し、 $(i_1..i_2)$  は  $i_1 < i < i_2$  なる整数  $i$  からなる集合 (区間) を表すものとする。

#### 【0233】

(順次集約木の構成方法)

・第  $l$  の順次集約木の構成方法

上述した基本関数の定義のもと、第  $l$  の動的な集約木の構成方法について説明する。この集約木の構成方法は、深さの違いを  $l$  以内に押さえ、ダミー・ノードを作成しない方法である。

#### 【0234】

集約期間 (例えば 1 週間) に受けけるイベント順序証明要求の数が何らかの方法により前以てさだまっているものとし、その数を  $n$  とする。このとき、集約木の高さ  $k$  は、 $k = \text{ceiling}(\log_2(N))$  である。高さ  $k$  の順次集約木リーフ数は最大で  $2^k$  であるので、 $d = 2^k - n$  として、レベル 0 のノードのうち、 $2^d$  個を消去すれば、イベント順序証明要求の数  $n$  をダミー・ノードなしでリーフに割り当てることが可能となる。これは、レベル 0 のリーフが  $2^d$  個減ると、レベル 1 のリーフが新たに  $d$  個できるので、合計で  $d$  個減り、リーフの数は結局、 $2^k - d = n$  となるからである。

#### 【0235】

以下、 $L1W = 2^{(k-1)}$  (レベル 1 のノードの個数)、 $L1L = 2^{(k-1)} - d$  (子を有するレベル 1 のノードの個数) の、 $L0L = 2^{(2^{(k-1)} - d)}$  (レベル 0 のノードの個数) とおくと、 $n$  個のイベント順序証明要求のうち、初めの  $L0L$  個をレベル 0 に配置し、残りをレベル 1 に配置するとき、 $i$  番目のイベント順序証明要求の配置先を表す関数  $\text{place}(i)$  は次式で表すことができる。

#### 【0236】

$$\text{place}(i) = (0, i) \quad (0 \leq i < L0L)$$

$$\text{place}(i) = (1, L1L + i - L0L) \quad (L0L \leq i \leq n)$$

ここで、 $\text{place}(i) = (\text{レベル}, \text{番号})$  で構成されているものである。

#### 【0237】

図 24 は、第 1 の動的な集約木の構成方法の  $n = 10$  の場合の具体例を示すものである。この場合においては、図 24 に示す通り、 $k = \text{ceiling}(\log_2(10)) = 4$  となり、高さは 4 である。そして、 $d = 2^4 - 10 = 6$  であるので、 $6 \times 2 = 12$  個のレベル 0 のリーフを消去する。この結果、 $L1W = 2^3 = 8$ 、 $L1L = 8 - 6 = 2$ 、 $L0L = 2 \times 2 = 4$  となる。従って、レベル 0 のリーフが 4 個、

レベル1のリーフが6個で、リーフの合計数は $n=10$ となる。この結果、図24に示すような集約木を動的に作成することができる。レベルが0より大きいノード（即ちリーフではないノード）に対する値の割当は、それが可能になったときにインクリメンタルに行われる。

#### 【0238】

##### ・第2の順次集約木の構成方法

次に、第2の動的な順次集約木の構成方法について説明する。この方法はインクリメンタルに集約木を構成する点では第1の方法と同じであるが、前もって定めた時間間隔（順次集約期間）に受付けるイベント順序証明要求の数は予想できないものと仮定している点が第1の方法と異なる。

#### 【0239】

ここで、インクリメンタルとは、イベント順序証明要求を受付ける都度、そこから計算できる順次集約木の部分を計算していくという意味である。以下では、受付けるイベント順序証明要求の数は予想できないが、その上界 $N$ は見積もることができるとして説明する。この方法においては、イベント順序証明要求はすべてレベル0に割り付けられるものと、二分木のルート値を計算するためにダミー・ノードを使用する方法である。

#### 【0240】

この方法で順次集約木を構成するとき、所定の集約期間（例えば、1週間）に受付けたイベント順序証明要求の数を $N$ とすると、順次集約木のの高さ $k$ は、 $k = \text{ceiling}(\log_2(N))$ である。高さ $k$ の順次集約木リーフ数は最大で $2^k$ であるので、0から $n-1$ までの $n$ 個のイベント順序証明要求をレベル0のノード $(0, 0)$ からノード $(0, n-1)$ に割り当てられることになる。

#### 【0241】

レベル0に割り当てられた、最も右のノード $(0, n-1)$ に対して、ルート・パス  $rtPath_k(0, n-1)$ が

$$rtPath_k(j, i) = [(j, r(j)), \dots, (k, r(k))]$$

と表現されるものとする。

#### 【0242】

（一般に、 $rtPath_k(j, i)$  は、 $rtPath_k(j, i) = [(j, r(j)), \dots, (k, r(k))]$ と表現される。但し、 $j \in [j, k]$  に対して  $r(j) = \text{floor}(i/2^{(j-1)})$ とする。）  
このとき、各レベル $j$  ( $j=0, \dots, k-1$ ) においては、以下のことが成り立つ。

#### 【0243】

$r(j)$ が偶数のとき、ノード $(j, r(j)+1)$ はダミー・ノードとなり、  
 $r(j)+1 \leq i < 2^{(k-j)}$ となる各 $i$ に対して、ノード $(j, i)$ は消去されている。

#### 【0244】

$r(j)$ が奇数のとき、 $r(j)+1 \leq i < 2^{(k-j)}$ となる各 $i$ に対して、ノード $(j, i)$ は消去されている。

#### 【0245】

以上のような方法に基づいて構成される順次集約木は、ダミー・ノードは各レベルの右端でのみ現れる、および作成されるダミー・ノードの数は、 $k$ 以下であるという性質を有する。

#### 【0246】

図25及び 図26は、第2の順次集約木の構成方法のアルゴリズムを示すものであり、該アルゴリズムに従って順次集約木がインクリメンタルに構成されるようになっている。ここで、前提として以下の定義を行う。

#### 【0247】

・ $K = \text{ceiling}(\log_2(N))$ とする。

#### 【0248】

・ $n$ は受付けたイベント順序証明要求の数を示す整数変数とする。初期値は0である。

#### 【0249】

・  $k$  は定められた時間間隔が終了したときの順次集約木の高さを表す変数とする。

【0250】

( $K+1$ ) 個のカウンタの列を、 $i_0, \dots, i_K$  とする。ここで、 $i_j$  の初期値は 0 である ( $j=0, \dots, K$ )。  $i_j$  はレベル  $j$  において、既に生成されたノードの数を表すと同時に、次にレベル  $j$  に作成されるノードの番号を表す。

【0251】

・ ( $K+1$ ) 個のブール変数の列を、 $b_0, \dots, b_K$  とする。ここで、 $b_j$  の初期値は false である ( $j=0, \dots, K$ )。  $b_j$  は、レベル  $j$  にダミー・ノードがあるか否かを表す。

【0252】

・ ( $K+1$ ) 個の配列の列を、 $A_0, \dots, A_K$  とする。各配列は、 $2^{(K-j)}$  の長さを持ち、レベル  $j$  のノードに割り付けられる値を保持する ( $j=0, \dots, K$ )。

【0253】

・  $r$  はダミー・ノードに割り当てるダミー値を保存する変数である。

【0254】

・  $R(j, i)$  は 2 つの引数  $i, j$  に対してノード  $(j, i)$  に割り当てるべきダミー値を計算する関数である。

【0255】

・  $x, x_0, x_1, x_2$  は、ノードに割り当てる値を表す変数である。

【0256】

・  $x_1 \parallel x_2$  は、ビット列で表された 2 つの値の接続である。

【0257】

・  $h(x)$  は  $x$  のハッシュ値を計算する衝突困難一方向ハッシュ関数である。

【0258】

このような定義のもと、図 25 の処理手順 1 が終了すると (即ち所定の順次集約期間が終了すると)、 $n$  は受付けた時刻処理要求の数、 $k$  は生成された順次集約木の高さ、 $i_j$  はレベル  $j$  のノードの数、 $b_j$  はレベル  $j$  にダミー・ノードがあるか否か、 $A_j$  は、レベル  $j$  のノードに割り付けられた値からなる配列をそれぞれ表すことになる。

【0259】

図 27 は、第 2 の動的な順次集約木の構成方法の  $n=9$  の場合の具体例を示す図である。即ち、定められた順次集約期間が終了したとき、 $n=9$  であったとする。このとき、 $k = \text{ceiling}(\log_2(9)) = 4$  となり、高さは 4 の順次集約木を構成することになる。尚、0 から  $n-1$  までの  $n$  個の順序証明要求は、処理手順 1 により、既にノード  $(0, 0), \dots, (0, n-1)$  に割り当てられている。また、処理手順 1 により、 $i_0=9, i_1=4, i_2=2, i_3=1, i_4=0$  となっている。

【0260】

このとき、処理手順 2 の (2.2) から、ノード  $(0, 8)$  のノートパス  $\text{rtPath}_4(0, 8)$  は

$$\text{rtPath}_4(0, 8) = [(0, 8), (1, 4), (2, 2), (3, 1), (4, 0)]$$

となる。これから、各レベルの手順は、以下の通りになる。

【0261】

レベル 0 においては、ステップ (2.3.2.1) より、ノード  $(0, 9)$  がダミー・ノードになる。レベル 1 においては、ステップ (2.3.3.1.5) より、ノード  $(1, 4)$  に値が割り付けられ、 $(1, 5)$  がダミー・ノードになる。レベル 2 においては、ステップ (2.3.3.1.5) より、ノード  $(0, 2)$  に値が割り付けられ、 $(0, 3)$  がダミー・ノードになる。レベル 3 においては、ステップ (2.3.3.1) により、ノード  $(3, 1)$  に値が割り付けられる。レベル 4 においては、ステップ (2.3.3.1) により、ノード  $(4, 0)$  に値が割り付けられる。

【0262】

この結果、図 27 に示すような順次集約木をインクリメンタルに構成することができる。ダミー・ノードは各レベルに於いて高々 1 つである。ダミー・ノードには前以て定められた何らの手順に従いダミー・ラベル (ダミー割当値) を割当てる必要があるが、このような手順の簡単な定義としては、レベルの関数としてダミー・ラベルを定義する方法があり



、これを採用してもよい。

図28は、上記のインクリメンタルな順次集約木の構成方法において各ノードに値を割付けるタイミングを示したものである。

#### 【0263】

上述の第1及至第3の実施の形態においては、順次集約木は図28に示すように、情報公表の区切りにおいては、ダミー・ノードを用いて最終的な順次集約木の構成する方式を前提としている。しかし、順次集約木の具体的な構成法としてこれ以外の方法を採用することも可能である。

#### 【0264】

即ち、上記実施の形態におけるイベント順序証明システム100、200及び300は、上述した動的な集約木の構成方法のいずれをも採用できるものであり、これにより、利用者装置からのイベント順序証明要求の量的変化に柔軟に対応することができるので、スケーラビリティの高いイベント順序証明システムを構築することが可能となる。

#### 【0265】

(認証パスの定義とそれによるルート値の計算法)

予め高さが決定しておらずインクリメンタルに構成されるような順次集約木のノードに対して、ある時点のルート・パスや認証パスを以下のように定義することができる。この定義は第1及至第3の実施の形態において所定の順次集約期間に受付ける要求の数が前以て予想できないときに適用することができる。

#### 【0266】

現時点のリーフ番号の最大値が $m (\geq 0)$  (従ってリーフの数が  $m+1$ ) のとき、

$$\kappa(m) = \min\{h \mid m+1 \leq 2^h\} \text{ とおく。}$$

高さが  $\kappa(m)$  の順次集約木を

$$\text{curSBT}(m)$$

と置く。

#### 【0267】

$p = (j, i) \in \text{curSBT}(m)$  とし、 $p$  から  $\text{curSBT}(m)$  のルートに至るノードの並びルート・パスと言いを

$$\text{rtPath}(p, m)$$

と書く。

#### 【0268】

$\text{rtPathD}(p, m)$  は、 $\text{rtPath}(p, m)$  に属するノードのうちで $m$ 番目のリーフの割当値が定まった時点で割当値が定まっている ノード の列である。

#### 【0269】

$$\text{rtPath}(p, m) = [(0, i(0)), \dots, (k, i(k))]$$

としたとき、 $0 \leq k_1 \leq k$  なるある $k_1$  があって、

$$\text{rtPathD}(p, m) = [(0, i(0)), \dots, (k_1, i(k_1))]$$

となることが分かる。

#### 【0270】

$\text{rtPathDV}(p, m)$  は、 $\text{rtPathD}(p, m)$  の各ノードに割当値を割り当てたものである。

#### 【0271】

$$\text{rtPathD}(p, m) = [(0, i(0)), \dots, (k_1, i(k_1))]$$

のとき、 $\text{rtPathDV}(p, m)$  は次のような形となる。

#### 【0272】

$$\text{rtPathDV}(p, m) = [(0, i(0)), v(0), \dots, (k_1, i(k_1)), v(k_1)]。$$

#### 【0273】

$\text{curSBT}(m)$  における、ノード  $p = (j, i)$  から $\text{curSBT}(m)$ のルート値を計算するのに必要なノード $p' = (j', i')$ の集合を該ノードの認証パスと呼び $\text{authPathT}(p, m)$ と表す。但し、認証パスに属する各ノードについて、該ノードを接続する方向(左又は右)についての情報もタグとして含んでいるものとする。

【0274】

$\kappa(m) = k$  で、

$$rtPath(p, m) = [(j, r(j)), \dots, (k, r(k))]$$

のとき、 $authPathT(p, m)$  は  $rtPath(p, m)$  を用いて次のように表すことができる。

【0275】

$$authPathT(p, m) =$$

$$[(j, a(j)), LR(j)), \dots, ((k-1, a(k-1)), LR(k-1))]$$

ここで、 $r(j')$  が偶数の場合、 $a(j') = r(j') + 1$ 、 $r(j')$  が奇数の場合、 $a(j') = r(j') - 1$  であり、また、 $r(j')$  が偶数の場合、 $LR(j') = R$ 、 $r(j')$  が奇数の場合、 $LR(j') = L$  である（但し、 $j' \in [j, k-1]$ ）。

【0276】

そして、 $authPathT(p, m)$  の要素  $((j, a(j)), LR(j))$  について、 $LR(j)$  の部分を (LR) タグという。さらに、 $rtPath(p, m)$  の要素  $(j, r(j))$  について、 $r(j)$  が偶数のとき、 $(j, r(j) + 1)$  を  $(j, r(j))$  の右補完点といい、 $r(j)$  が奇数のとき、 $(j, r(j) - 1)$  を  $(j, r(j))$  の左補完点という。

【0277】

このとき、 $authPathT(p, m)$  は、 $rtPath(p, m)$  のルート以外の点の右補完点あるいは左補完点からなる。

【0278】

また  $authPathT(p, m)$  から LR タグの情報を除いたものを  $authPath(p, m)$  と書く。即ち、

$$authPath(p, m) =$$

$$[(j, a(j)), \dots, ((k-1, a(k-1)))]$$

であるとき、

$$authPath(p, m) = [(j, a(j)), \dots, ((k-1, a(k-1)))]$$

とする。逆に

$$authPath(p, m) = [(j, a(j)), \dots, ((k-1, a(k-1)))]$$

が与えられれば  $authPathT(p, m)$  を以下のように計算できる。 $j_l \in [j, k]$  に対して、 $rtPath(p, m)$  のレベル  $j_l$  のノードは

$$(j_l, \text{floor}(i/2^{(j_l-j)}))$$

となるので、 $\text{floor}(i/2^{(j_l-j)})$  が偶数であるとき  $LR(j_l) = R$ 、奇数であるとき  $LR(j_l) = L$  と定め、

$$authPathT(p, m) =$$

$$[(j, a(j)), LR(j)), \dots, ((k-1, a(k-1)), LR(k-1))]$$

とおけばよい。従って、 $authPathT(p, m)$  と  $authPath(p, m)$  の一方から他方を計算することが出来る。

【0279】

$authPath(p, m)$  及び  $authPathT(p, m)$  の中で、 $m$  番目のリーフの割当値が定まった時点で割当値が定まっているノードの集まりを各々

$$authPathD(p, m) \text{ 及び } authPathTD(p, m)$$

と定義する。 $authPath(p, m)$  及び  $authPathT(p, m)$  が上記のように表現されるとき、

$$k_l \leq k - j \text{ なる } k_l \text{ と、}$$

$$j \leq j(0) < j(1) < \dots < j(k_l - 1)$$

なる非負整数  $j(0), \dots, j(k_l - 1)$  があり、

$$authPathD(p, m) = [(j(0), a(j(0))), \dots, (j(k_l - 1), a(j(k_l - 1)))],$$

$$authPathTD(p, m) = [(j(0), a(j(0))), LR(j(0))], \dots, (j(k_l - 1), a(j(k_l - 1))), LR(j(k_l - 1))],$$

と表現される。

【0280】

さらに、 $\text{authPathD}(p, m)$  及び  $\text{authPathTD}(l, m)$  に、それに属するノードの割当値を加えたものを、各々  $\text{authPathDV}(p, m)$  及び  $\text{authPathTDV}(p, m)$  と置く。具体的には、 $\text{authPathD}(p, m)$  及び  $\text{authPathTD}(p, m)$  が上記のように表現されるとき、

$$\begin{aligned} \text{authPathDV}(p, m) &= \\ &[ ((j(0), a(j(0))), v(j(0))), \dots, \\ &\quad ((j(kl-1), a(j(kl-1))), v(j(kl-1))) ], \\ \text{authPathTDV}(p, m) &= \\ &[ ((j(0), a(j(0))), LR(j(0)), v(j(0))), \dots, \\ &\quad ((j(kl-1), a(j(kl-1))), LR(j(kl-1)), v(j(kl-1))) ] \end{aligned}$$

とおく。ここで、各  $j' \in \{j(0), \dots, j(kl-1)\}$  に対して、 $v(j') = V(j', a(j'))$  である。

#### 【0281】

上述の順次集約木の構成法の何れかの方法により、リーフ番号  $m$  のリーフに順次割当値を割り当てた段階で当該の順次集約木の構成が終了し、かつ  $\text{authPathTDV}(p, m)$  が上記のように表されるとき、ノード  $p = (j, i)$  の割当値  $V(p)$  と  $\text{authPathTDV}(p, m)$  から以下のようにして集約木のルート値を計算することができる。 $j_1 \in [j, k]$  に対して、 $v'(j_1)$  を以下 (1), (2) により再帰的に定義する。このとき、 $v'(k)$  が集約木のルート値となる。

#### 【0282】

- (1)  $v'(j) = V(j, i)$
- (2)  $j_1 \in [j, k]$  に対して、 $v'(j_1)$  が定義されたとする、 $LR(j_1) = L$  のとき、  
 $v'(j_1+1) = h(v(j_1) \parallel v'(j_1))$   
 $LR(j_1) = R$  のとき、  
 $v'(j_1+1) = h(v'(j_1) \parallel v(j_1))$   
と定義する。

#### 【0283】

$m_1, m_2$  を順次集約木リーフ番号とし、 $m_1 \leq m_2$  とする。このとき、  
 $\text{curSBT}(m_1) \subseteq \text{curSBT}(m_2)$  である。

#### 【0284】

$p = (j, i) \in \text{curSBT}(m_1)$  とする。このとき、以下の (1), (2), (3) が成立つ。

#### 【0285】

- (1)  $\text{rtPath}(p, m_1) \subseteq \text{rtPath}(p, m_2)$
- (2)  $\text{authPath}(p, m_1) \subseteq \text{authPath}(p, m_2)$
- (3)  $\text{authPathD}(p, m_1) \subseteq \text{authPathD}(p, m_2)$

<順次集約木の諸性質>

以下では、インクリメンタルに構成される順次集約木について、現時点のリーフ番号の最大値を  $m$  とし、

$$\text{rtPath}((0, i), m), \text{rtPathD}((0, i), m), \text{rtPathDV}((0, i), m)$$

を各々短く

$$\text{rtPath}(i, m), \text{rtPathD}(i, m), \text{rtPathDV}(i, m)$$

と書くこともある。同様に

$$\begin{aligned} &\text{authPath}((0, i), m), \text{authPathT}((0, i), m), \text{authPathD}((0, i), m), \\ &\text{authPathTD}((0, i), m), \text{authPathDV}((0, i), m), \text{authPathTDV}((0, i), m) \end{aligned}$$

を各々短く

$$\begin{aligned} &\text{authPath}(i, m), \text{authPathT}(i, m), \text{authPathD}(i, m), \\ &\text{authPathTD}(i, m), \text{authPathDV}(i, m), \text{authPathTDV}(i, m) \end{aligned}$$

と書くこともある。

#### 【0286】

次に、順次集約木において、ユーザ点の監査点による認証点を計算するアルゴリズムについて説明する。前提として、順次集約木の高さを  $k$  とし、ユーザ点の識別番号を  $i_0$ 、監

査点の識別番号を  $i_l$  とし、 $i_0 < i_l$  とする。一般に、順次集約木のノード  $(0, i)$  に対して  $rtPath((0, i), m)$  は以下のように計算できる。

【0287】

$rtPath((0, i), m) = [(0, r(0)), \dots, (k, r(k))]$

但し、 $k = \kappa(m)$ 、 $j \in [0..k]$  に対して  $r(j) = \text{floor}(i/2^j)$  と置く。

【0288】

この手順によって、ノード  $(0, i_0)$  のルート・パス  $rtPath((0, i_0), m)$  とノード  $(0, i_l)$  のルート・パス  $rtPath((0, i_l), m)$  を計算する。すると、 $rtPath((0, i_0), m)$  と  $rtPath((0, i_l), m)$  は、ある要素以降は一致する。このとき、最初に一致した要素を、ノード  $(0, i_0)$  とノード  $(0, i_l)$  の合流点 (confluent point) と呼ぶ。そして、合流点のレフト・チャイルドを、ノード  $(0, i_0)$  (ユーザ点) のノード  $(0, i_l)$  (監査点) による認証点 (authentication point) とよぶ。

【0289】

以上は、ユーザ点と監査点が同一の順次集約木に属する場合における認証点の定義であるが、該ユーザ点が属する順次集約木 SBT より後に、該監査点の属する順次集約木の属する順次集約木が生成される場合には、SBT のルートを該ユーザ点の該監査点による認証点と定義する。

【0290】

(順次集約木の性質1)

B をある順次集約木の部分順次集約木で、ある時点において、 $\text{last}(\text{leaves}(B))$  に対応するラウンドの処理が終了済みとする。このとき、その時点において B に属する各ノードの割当値は計算され割当てられている。

【0291】

・性質1の証明

図25及び図26で示されるインクリメンタルな順次集約木の構成法により、各ラウンドの終了時には、そのラウンドまでに取得できたリーフの割当値により計算できるリーフ以外のノードの割付値は全て計算され該ノードに割当てられることになる。

【0292】

$\text{last}(\text{leaves}(B))$  に対応するラウンドの処理が終了したときには、 $\text{leaves}(B)$  に属する各リーフの割当値は定まっており、従って B の各ノードの割当値が計算できる。従って、この段階で、B の各ノードの割当値は計算され、各ノードに割当てられている。

予め高さが決定しておらずインクリメンタルに構成されるような順次集約木に対して、次の性質2がなりたつ。

【0293】

(順次集約木の性質2)

C を利用者装置、Z を監査装置とし、 $i_0$  と  $i_l$  を  $i_0 < i_l$  なる二つの順次集約木リーフ番号とし、 $\text{round}(i_0)$  において、C は受理証明書を受信し、Z は  $\text{round}(i_l)$  において監査用受理証明書を受信したものとする。このとき、 $i_0$  の  $i_l$  による認証点は以下の性質を持つ。

【0294】

(1) 認証点の割当値は、監査点、即ちノード  $(0, i_l)$  の受理証明書内補完データに含まれる。

【0295】

(2) 上記認証点を  $(j', i')$  とおくと、 $\text{authPath}((0, i_0), i_l)$  に属するノードで、レベルが  $j'$  より小さいものに対する割当値は、ノード  $(0, i_l)$  に対応するラウンドで受理証明書を受信した利用者が、ノード  $(0, i_l)$  に対応するラウンド以降において受信できる遅延補完データあるいは受信した受理証明書内補完データに含まれる。

【0296】

即ち、 $i_l \leq i_2$  とすると、 $\text{authPath}((0, i_0), i_l)$  に属するノードで、レベルが  $j'$  より小さいものに対する割当値は、 $\text{EOC}(i_0)$  あるいは  $\text{CToken}(i_0, i_2)$  に含まれる。

### 【0297】

(3) 上記認証点の割当値及び  $rtPath((0, i0), i2)$  に属するノードでレベルが該認証点のレベルより小さいノードの割当値は、ノード  $(0, i0)$  で受理証明書を受理した利用者が、ノード  $(0, i1)$  に対応するラウンド以降において受信する遅延補完データおよびノード  $(0, i0)$  で受信した受理証明書（受理証明書内補完データを含む）から計算することができる。

### 【0298】

・性質2の証明

以下では、利用者に渡す受理証明書に、受理証明書内補完データ（即時補完データ）を含める場合について説明する。利用者に渡す受理証明書に受理証明書内補完データを含めず、その代わりに遅延補完データにこの情報を含める場合でも同様の議論により同じ結論が得られる。

### 【0299】

(1) まず、項目(1)について図29を用いつつ説明する。ここで、合流点を  $(j, i)$ 、そのレフト・チャイルドである認証点を  $(j', i')$  とおく。ノード  $(0, i1)$  の  $curSBT(i1)$  におけるルート・パス  $rtPath((0, i1), i1)$  において、 $(0, i1)$  から出発して、合流点に至る直前のノードを  $(j'', i'')$  とおく。このとき、認証点は、 $(j', i')$  の左補完点である。従って、認証パス  $authPathT(i1, i1)$  の定義から、 $((j', i'), L)$  はノード  $(0, i1)$  の  $curSBT(i1)$  における認証パスに含まれる。また、ノード  $(j', i')$  への値の割当ては、 $round(i1)$  より前に終了している。よって、 $((j', i'), L, V(j', i'))$  は  $(0, i1)$  に対する受理証明書内補完データに含まれる。

### 【0300】

(2) 次に項目(2)について図30および図31を用いつつ説明する。

### 【0301】

$k = \kappa(i1)$  とおく。

### 【0302】

認証点  $(j', i')$  はノード  $(0, i0)$  のルート・パス  $rtPath((0, i0), i1)$  に含まれる。ここで、

$$rtPath((0, i0), i1) = [(0, r(0)), \dots, (j', r(j')), (j'+1, r(j'+1)), \dots, (k, r(k))]$$

とする。

### 【0303】

また、 $authPath((0, i0), i1)$  の要素で、レベルが  $j'$  より小さいノードの並びを

$$[(0, s(0)), \dots, (j'-1, s(j'-1))]$$

とおく。

### 【0304】

各  $j1 \in [0, j'-1]$  に対して、 $V(j1, r(j1))$  が  $EOC(i0)$  あるいは  $CToken(i0, i2)$  に含まれることを示せばよい。

### 【0305】

$authPath((0, i0), i1)$  の定義により、 $authPath((0, i0), i1)$  のレベル  $j1$  の要素  $p2 = (j1, s(j1))$  は、 $rtPath((0, i0), i1)$  のレベル  $j1+1$  の要素  $p3 = (j1+1, r(j1+1))$  のライト・チャイルドであるか或いはレフト・チャイルドである。どちらであるかによって場合分けする。

### 【0306】

(場合1)  $p2$  が  $p3$  のライト・チャイルドであるとき、図30に示すように、 $p2$  の割当値  $V(p2)$  は、 $i1 \leq i2$  な  $i2$  において、 $C$  が受信できる遅延補完データ  $CToken(i0, i2)$  に含まれる。なぜならば、順次集約木の性質1により、リーフ  $(0, i1)$  に対応するラウンドのイベント順序証明処理が終わった時点で、図30のBで表された  $curSBT(i1)$  の部分木の割当値は計算可能であり計算され割当て済みである。従って、その時点以降で発行される遅延補完データにはBのルート  $p2$  の割当値  $V(p2)$  が含まれる。

### 【0307】

(場合2)  $p2$ が $p3$ のレフト・チャイルドであるとき、図31に示すように、ノード $p2$ の割当値 $V(p2)$ は、 $\text{round}(i0)$ のイベント順序証明要求者に対するト受理証明書内補完データに含まれる。何故ならば、図31の $p2$ をルートとする部分木 $B$ について、

$$\forall i \in \text{leaves}(B) [i < i0]$$

であり、従って $B \subseteq \text{curSBT}(i0)$ でかつ $i0$ で識別されるラウンドの開始時に、 $\text{leaves}(B)$ の割当値は確定している。よって 順次集約木の性質1により、 $p2 = \text{root}(B)$ の割当値は、 $i0$ で識別されるラウンドにおいて確定している。従って、 $p2$ は $\text{authPathD}((0, i0), i0)$ に含まれる。

### 【0308】

(3) 認証パスの定義及び項目(2)から、各 $j1 \in [0..j']$ に対して、 $V(j1, r(j1))$ を以下のように再帰的に計算することが出来る。

### 【0309】

まず、 $V(0, r(0))$ はイベント受理証明書に含まれているノード $(0, i0)$ の割当値とする。

### 【0310】

次に、 $j1 \in [0..j'-1]$ に対して、 $V(j1, r(j1))$ が計算されたと仮定し、 $V(j1+1, r(j1+1))$ を以下のように計算する。 $r(j1) < s(j1)$ のときは、

$$V(j1+1, r(j1+1)) = h(V(j1, r(j1)) \parallel V(j1, s(j1)))$$

とし、 $s(j1) < r(j1)$ のときは、

$$V(j1+1, r(j1+1)) = h(V(j1, s(j1)) \parallel V(j1, r(j1)))$$

とする。

### 【0311】

以下では、時刻の原点として、イベント順序証明システムのサービス開始時点を取り、時間を計る単位として1秒、1ミリ秒等を定め、時刻を、上記の原点から上記の時間の単位で計った整数で表現するものとする。また、各監査装置 $\mathcal{Z}$ は、各順次集約期間 $T$ の最初の監査点においては、 $T$ に閉じた監査情報に加えて、前順次集約ルート値(直前の順次集約期間 $T'$ のルートの割当値 $V(\text{root}(T'))$ )も受信するものとする。

### 【0312】

予め高さが決定しておらずインクリメンタルに構成されるような順次集約木に対して次の性質3がなりたつ。

### 【0313】

(順次集約木の性質3)

以下では、 $T$ を正整数とし、 $\alpha, \alpha 0, \tau, \tau'$ は拡張リーフ識別子を表すものとする。 $\mathcal{Z}$ は監査装置とし、 $\mathcal{Z}$ の監査点 $\alpha 0$ で、次の条件(\*1)を満たすものが存在するものとする。

### 【0314】

(\*1)  $\text{time}(\alpha 0) \in [0..T)$

さらに $\mathcal{Z}$ による任意の1つの監査点を $\alpha$ 、その次の $\mathcal{Z}$ による監査点を $\alpha'$ とすると次の条件(\*2)が成り立つものとする。

### 【0315】

(\*2)  $\text{time}(\alpha') - \text{time}(\alpha) \leq T$

また、利用者 甲 はあるイベント順序証明要求を送信し、その要求に対応する順次集約木リーフを $\tau$ 、その後、該イベント受理証明書に対する遅延補完データ要求し、その要求に対応する順次集約木リーフを $\tau'$ とすると次の条件(\*3)が成り立つものとする。

### 【0316】

(\*3)  $\text{time}(\tau') - \text{time}(\tau) \geq T$

さらに、監査装置 $\mathcal{Z}$ は2番目以降の各順次集約期間に属する $\mathcal{Z}$ による最初の監査点において、直前の順次集約期間のルート値をイベント順序証明機関から受信するものとする。

### 【0317】

このとき、以下の(1)及至(4) が成り立つ。

【0318】

- (1)  $\alpha \in [\tau.. \tau']$  となる乙によるある監査点 $\alpha$ が存在する。
- (2)  $\alpha \in [\tau.. \tau']$  となる乙による監査点 $\alpha$ について、 $\tau$  の  $\alpha$  による認証点の割当値(ラベル)は、 $\alpha$  以後のある順次集約木リーフ(例えば $\tau'$ )において 乙 が受信する監査用受理証明書に含まれる。

【0319】

- (3) 任意の順次集約木リーフ $\tau$ に対して、乙による監査点 $\alpha'$ があり、次の条件(\*4)が成立つ。

【0320】

- (\*)4  $\text{time}(\tau) \leq \text{time}(\alpha') < \text{time}(\tau) + T$
- (4)  $T \leq \text{time}(\tau)$ となる任意のユーザ点 $\tau$ について、 $\alpha < \tau$ となる乙の監査点 $\alpha$ が存在する。

【0321】

・性質3の証明

- (1)  $\alpha \in [\tau.. \tau']$  となるような乙によるある監査点 $\alpha$ が存在しないと仮定する。 $\tau$ より左に位置する乙による監査点が存在するか否かにより場合分けする。

【0322】

(場合1)  $\tau$ より左に位置する乙による監査点が存在する場合を考える。 $\tau$ より左に位置し、 $\tau$ に最も近い乙による監査点を $\alpha_1$ とし、 $\tau'$ より右に位置しかつ $\tau'$ に最も近い乙による監査点を $\alpha_2$ とする。 $\alpha_1$ と $\alpha_2$ のとり方より、

$$\text{time}(\alpha_1) < \text{time}(\tau) \text{ 及び } \text{time}(\tau') < \text{time}(\alpha_2)$$

が成り立つ。 $\text{time}(\alpha_1) < \text{time}(\tau)$ より、 $-\text{time}(\alpha_1) > -\text{time}(\tau)$ となる。

【0323】

従って、

$$\text{time}(\alpha_2) - \text{time}(\alpha_1) > \text{time}(\tau') - \text{time}(\tau) \geq T.$$

一方、 $\text{time}(\alpha) \in [\text{time}(\tau).. \text{time}(\tau')]$ となるような乙によるある監査点 $\alpha$ が存在しないのであるから、 $\alpha_2$ は $\alpha_1$ の次の監査点である。従って上記条件(\*2)より、

$$\text{time}(\alpha_2) - \text{time}(\alpha_1) \leq T \text{ とならなければならない。以上から、}$$

$$\text{time}(\alpha_2) - \text{time}(\alpha_1) > T \text{ かつ } \text{time}(\alpha_2) - \text{time}(\alpha_1) \leq T$$

となり矛盾が導かれる。従って、 $\text{time}(\alpha) \in [\text{time}(\tau).. \text{time}(\tau')]$ となるような乙によるある監査点 $\alpha$ が存在しないという仮定は誤りであり、 $\text{time}(\alpha) \in [\text{time}(\tau).. \text{time}(\tau')]$ となる乙によるある監査点 $\alpha$ が存在する。

【0324】

(場合2)  $\tau$ より左に位置する乙による監査点が存在しない場合を考える。このとき、 $\text{time}(\alpha_0) \in [0..T]$ なる監査点 $\alpha_0$ について、

$$\alpha_0 \in [\tau.. \tau']$$

となることが示される。

【0325】

- (2) 上述の順次集約木の性質2と項目(1)から直ちに導かれる。

【0326】

- (3)  $\tau$ より前に乙の監査点が存在するか否かにより場合分けする。

【0327】

(場合1)  $\tau$ より前に乙の監査点が存在する場合を考える。 $\tau$ より前で、最も後に位置する監査点を $\alpha$ とし、その次の監査点の時刻を $\alpha'$ とする。このとき、

$$\text{time}(\alpha) < \text{time}(\tau) \leq \text{time}(\alpha')$$

従って、条件(\*2)より、

$$\text{time}(\alpha') - \text{time}(\tau) < \text{time}(\alpha') - \text{time}(\alpha) \leq T$$

よって、

$$\text{time}(\alpha') < \text{time}(\tau) + T$$

以上より、(\*4)が得られる。

【0328】

(場合2)  $\tau$  より前に乙の監査点が存在しない場合を考える。性質3の前提により、乙の監査点  $\alpha 0$  で  $\text{time}(\alpha 0) < T$  となるものがある。

【0329】

$$\text{time}(\tau) \leq \text{time}(\alpha 0) < T$$

従って、

$$\text{time}(\alpha 0) - \text{time}(\tau) < T - \text{time}(\tau) \leq T$$

よって、 $\text{time}(\alpha 0) < \text{time}(\tau) + T$

以上により、 $\alpha' = \alpha 0$  として、(\*4)が得られる。

【0330】

(4) 乙の監査点  $\alpha 0$  で、 $\text{time}(\alpha 0) \in [0..T)$  となるものが存在するという上記仮定(\*1)から、直ちに導かれる。

【0331】

(順次集約木の性質4)

SBTを高さ  $k$  の順次集約木とし、 $i$  を SBT の順次集約木リーフ番号とし、 $k! \leq k$  とし、 $\text{authPathT}_{k!}(i)$  を、 $\text{authPathT}(i)$  の最初の  $k!$  個の要素の列とする。

【0332】

$$\text{authPathT}_{k!}(i) = [((0, i(0)), \text{LR}(0)), \dots, ((k!-1, i(k!-1)), \text{LR}(k!-1))]$$

と置く。さらにここで、 $v1, v2$  を異なる2つのハッシュ値とし、 $AP1, AP2$  を次のように与える。

【0333】

$AP1 =$

$$[(\text{LR}(0), v1'(0)), (\text{LR}(1), v1'(1)), \dots, (\text{LR}(k!-1), v1'(k!-1))],$$

$AP2 =$

$$[(\text{LR}(0), v2'(0)), (\text{LR}(1), v2'(1)), \dots, (\text{LR}(k!-1), v2'(k!-1))].$$

このとき、 $v1$  と  $AP1$  から以下の(\*1)のようにに計算した  $v1''(k!)$  と、 $v2$  と  $AP2$  から以下の(\*2)のように計算した  $v2''(k!)$  は(実用上無視できる確率を除いて)一致しない。

【0334】

(\*1) 各  $j' \in [0..k!]$  に対して、 $v1''(j')$  を以下のように再帰的に定める。

【0335】

$$v1''(0) = v1.$$

【0336】

$j' > 0$  で  $\text{LR}(j'-1) = L$  のとき、

$$v1''(j') = h(v1'(j'-1) \parallel v1''(j'-1))$$

$j' > 0$  で  $\text{LR}(j'-1) = R$  のとき、

$$v1''(j') = h(v1''(j'-1) \parallel v1'(j'-1))$$

(\*2) 各  $j' \in [0..k]$  に対して、 $v2''(j')$  を以下のように再帰的に定める。

【0337】

$$v2''(0) = v2$$

$j' > 0$  で  $\text{LR}(j'-1) = L$  のとき、

$$v2''(j') = h(v2'(j'-1) \parallel v2''(j'-1))$$

$j' > 0$  で  $\text{LR}(j'-1) = R$  のとき、

$$v2''(j') = h(v2''(j'-1) \parallel v2'(j'-1))$$

・性質4の証明

$v1''(k!) = v2''(k!)$  と仮定する。 $j' \in [0..k!]$  で  $v1''(j') = v2''(j')$  となる最小の  $j'$  を  $j1$  と置く。 $v1 \neq v2$ 、即ち  $v1''(0) \neq v2''(0)$  であるから、 $j1 > 0$  である。 $j0 = j1 - 1$  と置く。 $\text{LR}(j0)$  が  $L$  であるか  $R$  であるかにより場合分けする。

【0338】

(場合1)  $\text{LR}(j0) = L$  のとき。 $j1, j0$  のとり方より、



$$v1''(j0) \neq v2''(j0)。$$

【0339】

従って、

$$v1'(j0) \parallel v1''(j0) \neq v2'(j0) \parallel v2''(j0)$$

一方、上述の(\*1), (\*2) から、

$$v1''(j1) = h(v1'(j0) \parallel v1''(j0))$$

$$v2''(j1) = h(v2'(j0) \parallel v2''(j0))$$

従って、

$$h(v1'(j0) \parallel v1''(j0)) = h(v2'(j0) \parallel v2''(j0))$$

従って、 $v1'(j0) \parallel v1''(j0)$ と $v2'(j0) \parallel v2''(j0)$ が、衝突困難ハッシュ関数  $h$ の衝突となる。

【0340】

(場合2)  $LR(j0) = R$  のとき、場合1に於けると同様にして、

$v1''(j0) \parallel v1'(j0)$ と $v2''(j0) \parallel v2'(j0)$ が、衝突困難ハッシュ関数  $h$ の衝突となることが導かれる。

【0341】

以上から、どちらの場合でも、衝突困難ハッシュ関数  $h$ の衝突が現れることになる。このようなことは(実用上無視できる確率を除いて)在り得ない。従って、 $v1''(k) = v2''(k)$ となることも、(実用上無視できる確率を除いて)在り得ない。

【図面の簡単な説明】

【0342】

【図1】本発明の第1の実施の形態に係るイベント順序証明システムのシステム構成図である。

【図2】本発明の第1の実施の形態に係るイベント順序証明システムの別のシステム構成図である。

【図3】本発明に用いられる順次集約木の構成を説明する図である。

【図4】本発明におけるイベント順序受理証明書の構成を説明する図である。

【図5】本発明に用いられる順次集約木の認証パスを説明する図である。

【図6】本発明の第1の実施の形態に係るイベント順序証明システムのイベント順序証明方法を説明するシーケンス図である。

【図7】本発明の第1の実施の形態に係るイベント順序証明システムのイベント順序証明検証方法を説明するシーケンス図である。

【図8】本発明の第1の実施の形態に係るイベント順序証明システムのイベント順序証明検証方法を説明するシーケンス図である。

【図9】本発明の第1の実施の形態に係るイベント順序証明システムにおけるユーザ点と監査点の関係を説明する図である。

【図10】本発明の第1の実施の形態に係るイベント順序証明システムのイベント順序証明検証結果を説明する図である。

【図11】本発明の第2の実施の形態に係るイベント順序証明システムのシステム構成図である。

【図12】本発明の第2の実施の形態に係るイベント順序証明システムにおけるユーザ点と監査点の関係を説明する図である。

【図13】本発明の第2の実施の形態に係るイベント順序証明システムのイベント順序証明方法を説明するシーケンス図である。

【図14】本発明の第2の実施の形態に係るイベント順序証明システムのイベント順序証明検証方法を説明するシーケンス図である。

【図15】本発明の第2の実施の形態に係るイベント順序証明システムの2ユーザ間の順序を判定する動作を説明するフローチャート図である。

【図16】本発明の第2の実施の形態に係るイベント順序証明システムの複合完全化によるルート値検証の動作を説明するフローチャート図である。

【図 1 7】本発明の第 2 の実施の形態に係る イベント 順序 証明 システム の 補完 データ 完全化を説明する図である。

【図 1 8】本発明の第 2 の実施の形態に係る イベント 順序 証明 システム の 補完 データ 完全化を説明する図である。

【図 1 9】本発明の第 3 の実施の形態に係る イベント 順序 証明 システム の システム 構成 図 である。

【図 2 0】本発明の第 3 の実施の形態に係る イベント 順序 証明 システム の イベント 順序 証明 方法 の イベント 順序 証明 要求 ステップ を 説明 する シーケンス 図 である。

【図 2 1】本発明の第 3 の実施の形態に係る イベント 順序 証明 システム の イベント 順序 証明 方法 の イベント 順序 証明 要求 ステップ を 説明 する シーケンス 図 である。

【図 2 2】本発明の第 3 の実施の形態に係る イベント 順序 証明 システム の イベント 順序 証明 方法 の 監査 用 受理 証明書 受信 ステップ を 説明 する シーケンス 図 である。

【図 2 3】本発明の第 3 の実施の形態に係る イベント 順序 証明 システム の イベント 順序 証明 検証 方法 の 区間 時刻 証明書 ステップ を 説明 する シーケンス 図 である。

【図 2 4】深さの違いを 1 以内に抑さえ、ダミーノードを作成しない動的な順次集約木の構成方法を説明する図である。

【図 2 5】インクリメンタルに順次集約木を構成する方法のアルゴリズムを説明する図である。

【図 2 6】インクリメンタルに順次集約木を構成する方法のアルゴリズムを説明する図である。

【図 2 7】インクリメンタルに順次集約木を構成する方法を説明する図である。

【図 2 8】インクリメンタルに順次集約木を構成する方法において各ノードに値を割付けるタイミングを説明する図である。

【図 2 9】認証点の割当値は、監査点の受理証明書内補完データに含まれることを説明する図である。

【図 3 0】認証点のレベルより低い認証パスノードは、遅延補完データあるいは受理証明書内補完データに含まれることを説明する図である。

【図 3 1】認証点のレベルより低い認証パスノードは、遅延補完データあるいは受理証明書内補完データに含まれることを説明する図である。

【図 3 2】イベント順序証明システム の 概念 を 説明 する 図 である。

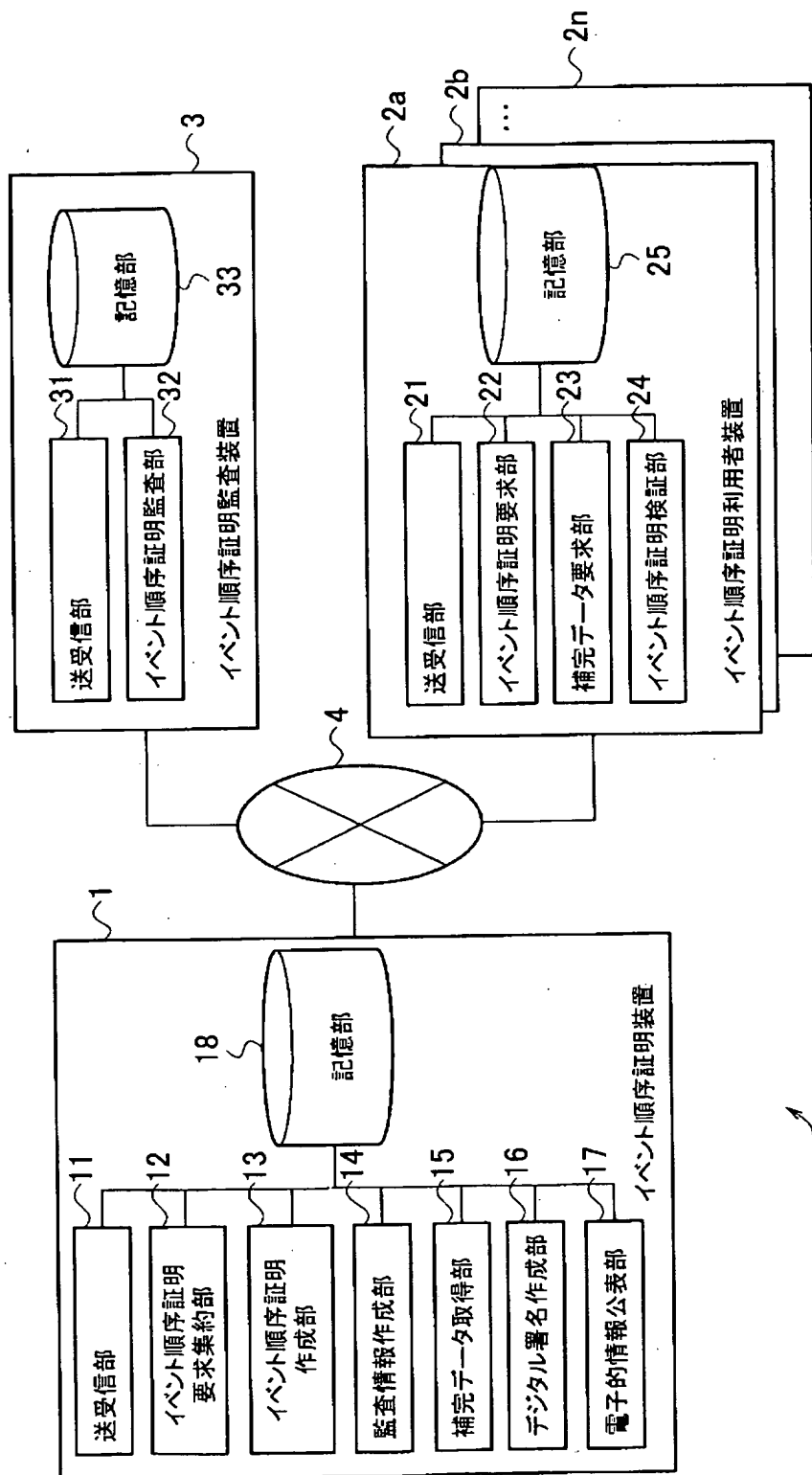
【図 3 3】線形リンクを用いたイベント順序証明システム の 概念 を 説明 する 図 である。

#### 【符号の説明】

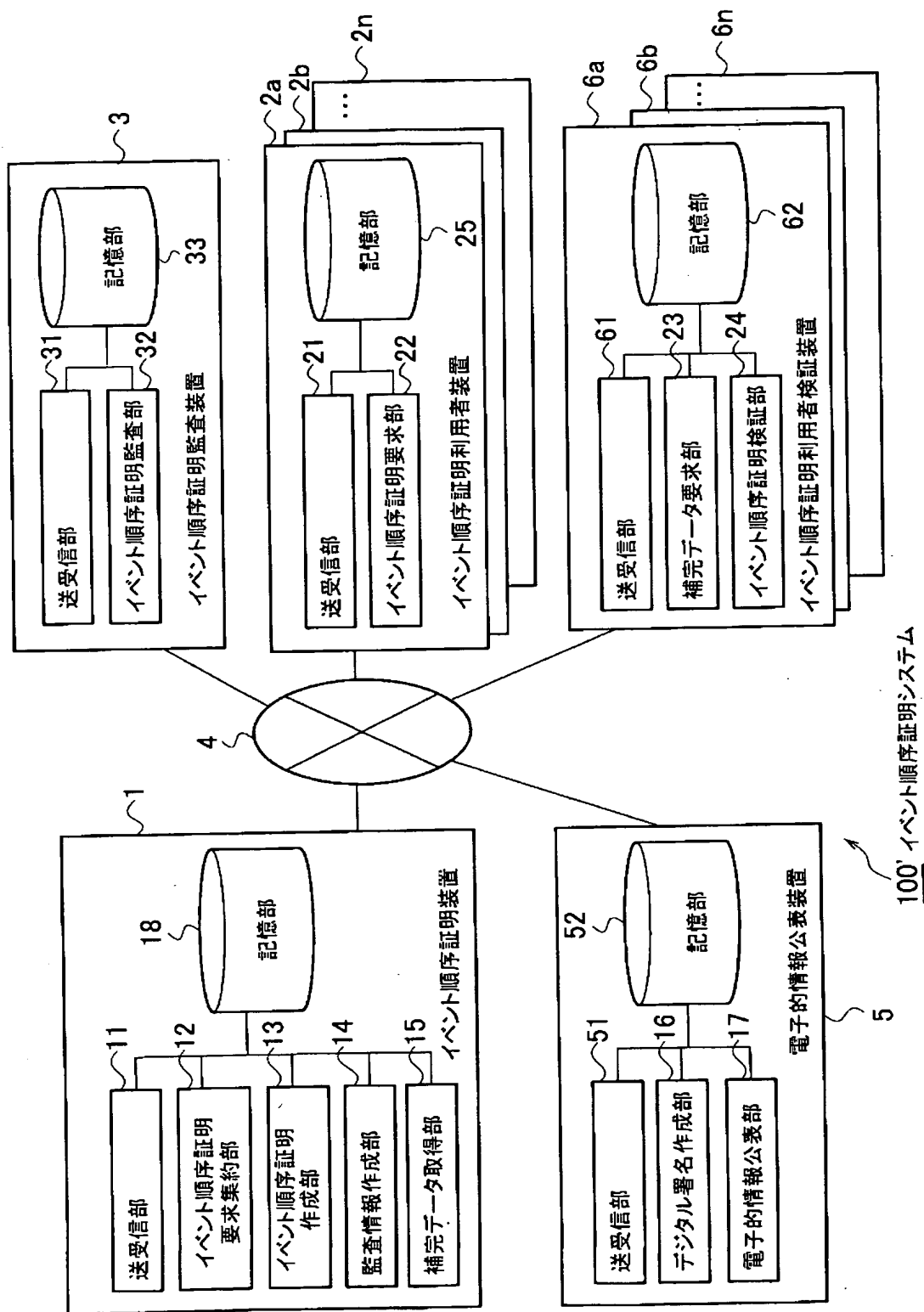
##### 【0343】

- 1, 7, 90 … イベント 順序 証明 装置
- 2 i … イベント 順序 証明 利用者 装置
- 3, 8 … イベント 順序 証明 監査 装置
- 4 … コンピュータ ネットワーク
- 5 … 電子的 情報 公表 装置
- 6 … イベント 順序 証明 利用者 検証 装置
- 9 … イベント 順序 証明 監査 装置 & イベント 時刻 監査 装置
- 10 j … 時刻 証明 利用者 装置
- 11, 21, 31, 51, 61 … 送受信部
- 12 … イベント 順序 証明 要求 部
- 13 … イベント 順序 証明 作成 部
- 14, 71 … 監査 情報 作成 部
- 15 … 補完 データ 取得 部
- 16 … デジタル 署名 作成 部
- 17 … 電子的 情報 公表 部
- 18, 25, 33, 52, 62, 72, 83, 92, 204 … 記憶 部

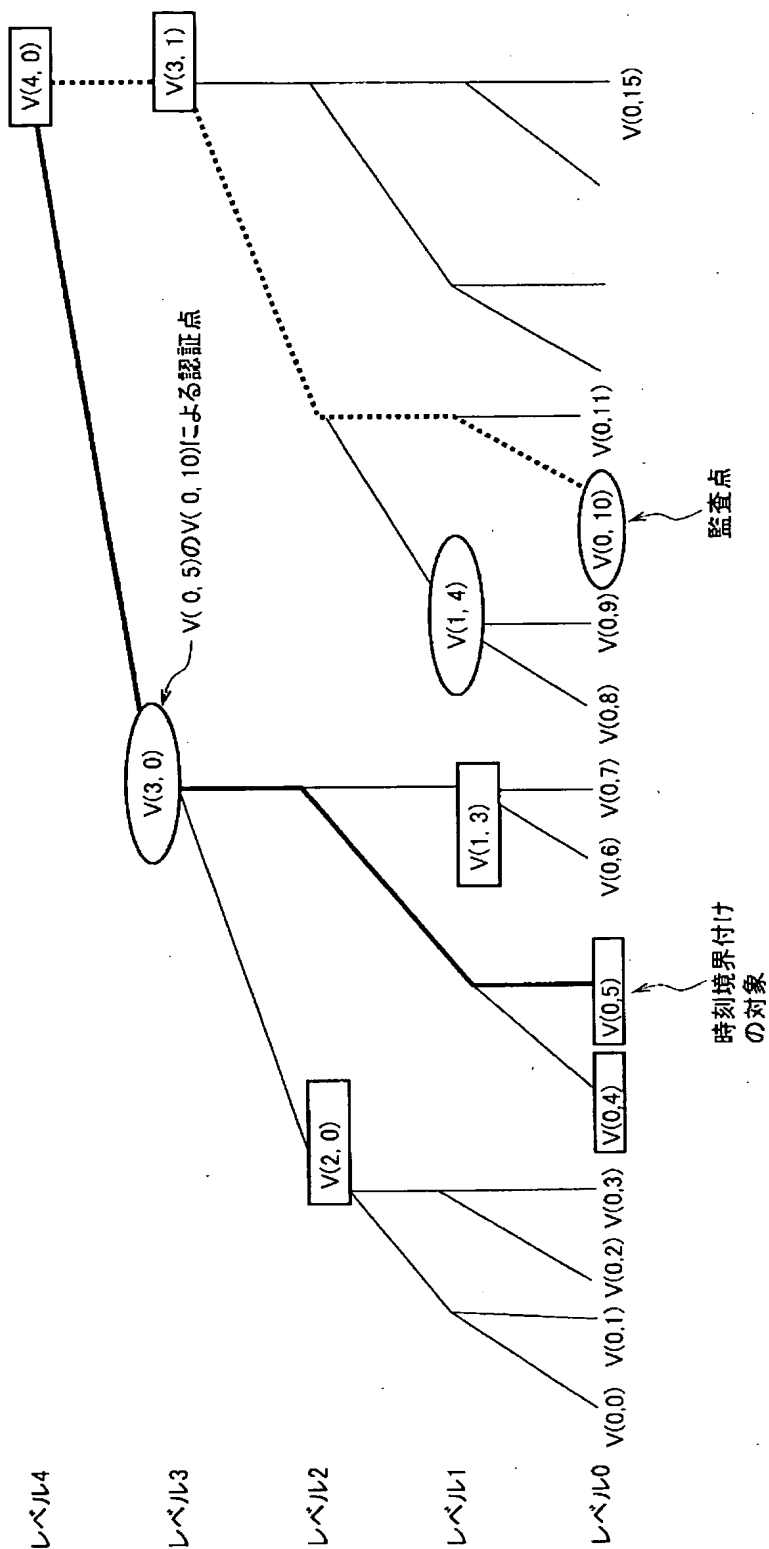
20 i ... イベント順序証明利用者装置&時刻証明装置  
22, 202 ... イベント順序証明要求部  
23 ... 補完データ要求部  
24, 203 ... イベント順序証明検証部  
30 ... 時刻情報提供装置  
32, 82 ... イベント順序証明監査部  
80 ... 利用者  
81 ... 補完データ要求部  
91 ... 区間時刻証明証作成部  
100, 200, 300, 900, 910 ... イベント順序証明システム  
201 ... 時刻証明作成部



【図2】



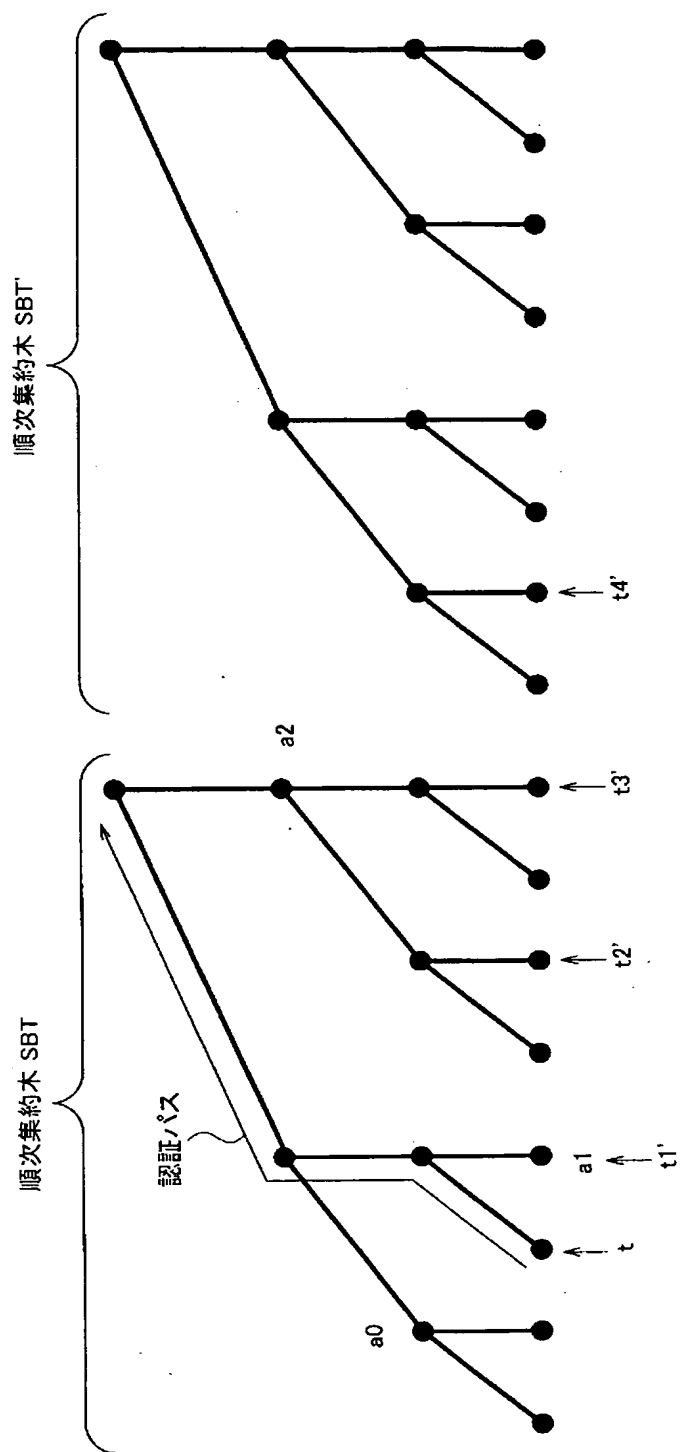
100 イベント順序証明システム



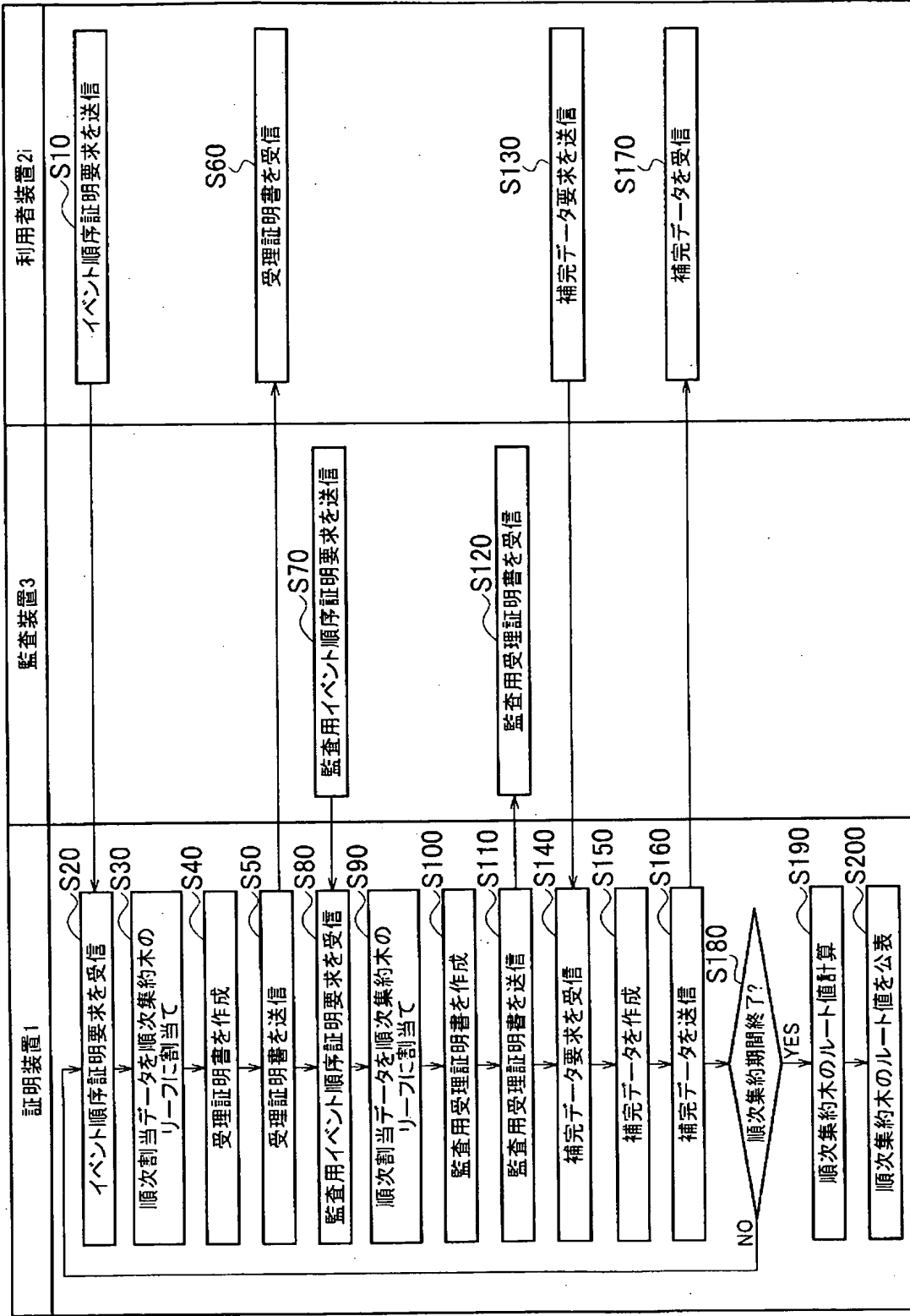
【 図 4 】

項目	記号	必須
元デジタルデータ	y	○
順次割当データ	z	○
順次集約木番号	n	○
順次集約木リーフ番号	i	○
即時補完データ(位置情報、割当値)	HK	
デジタル署名	DS	

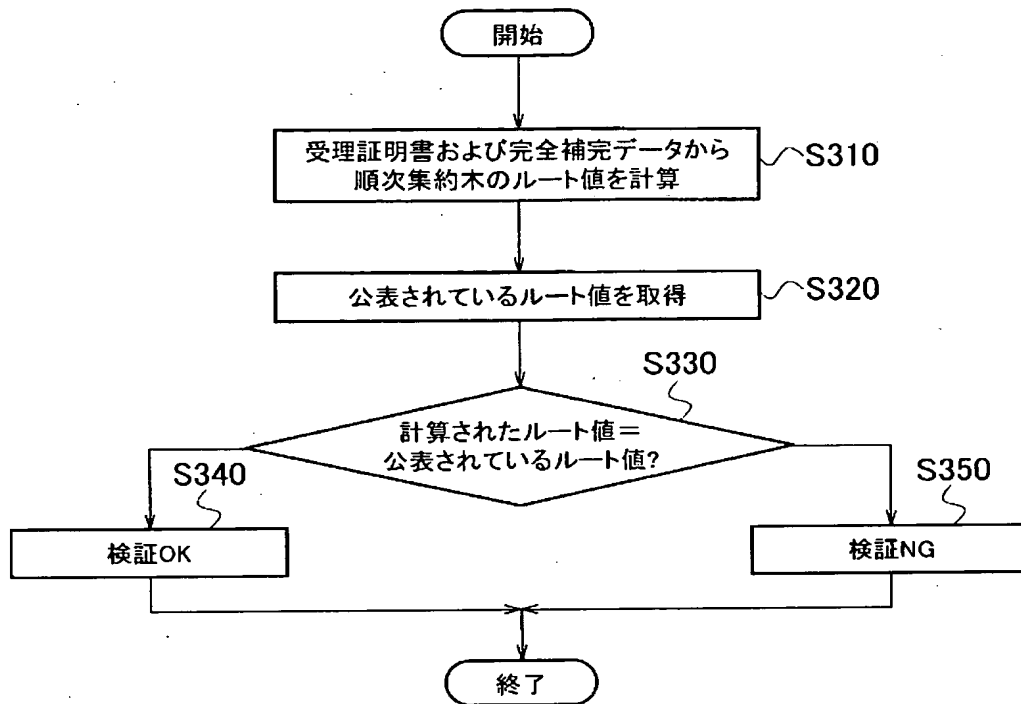
【図 5】

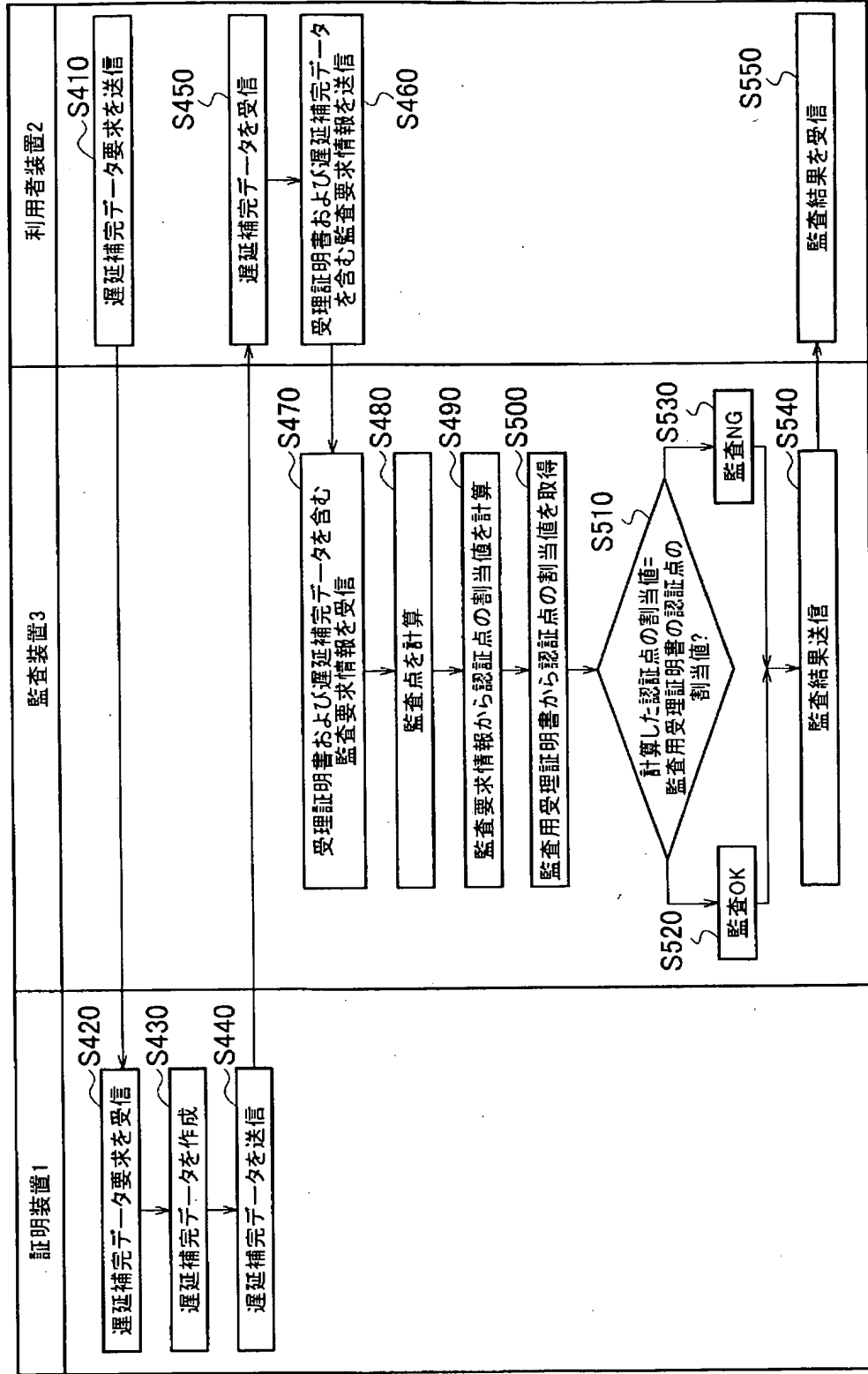




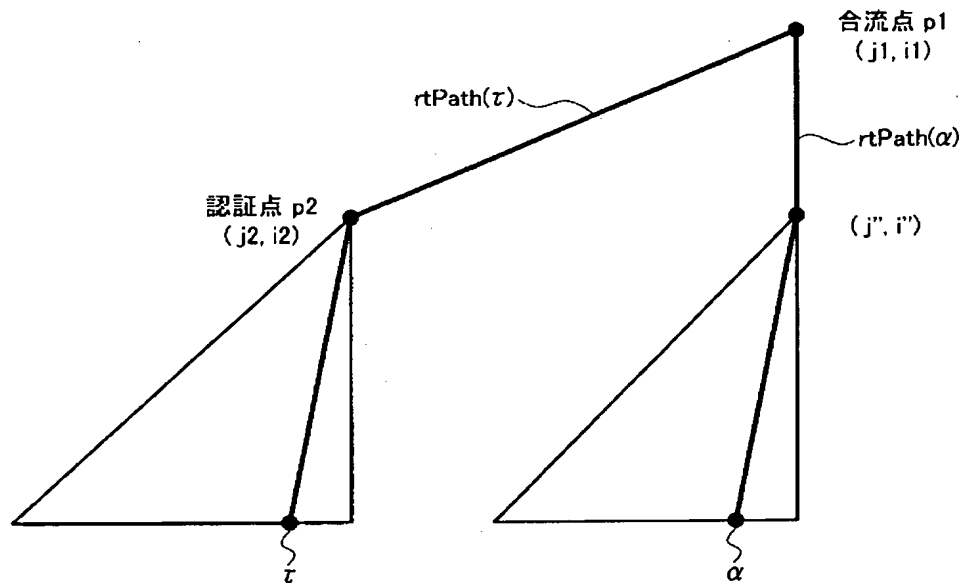


【図 7】

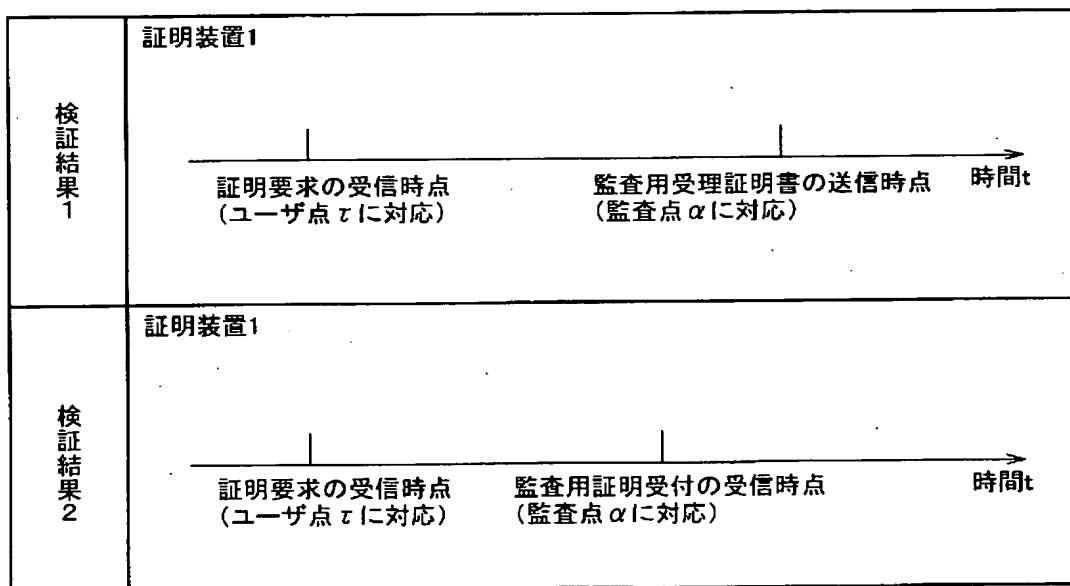


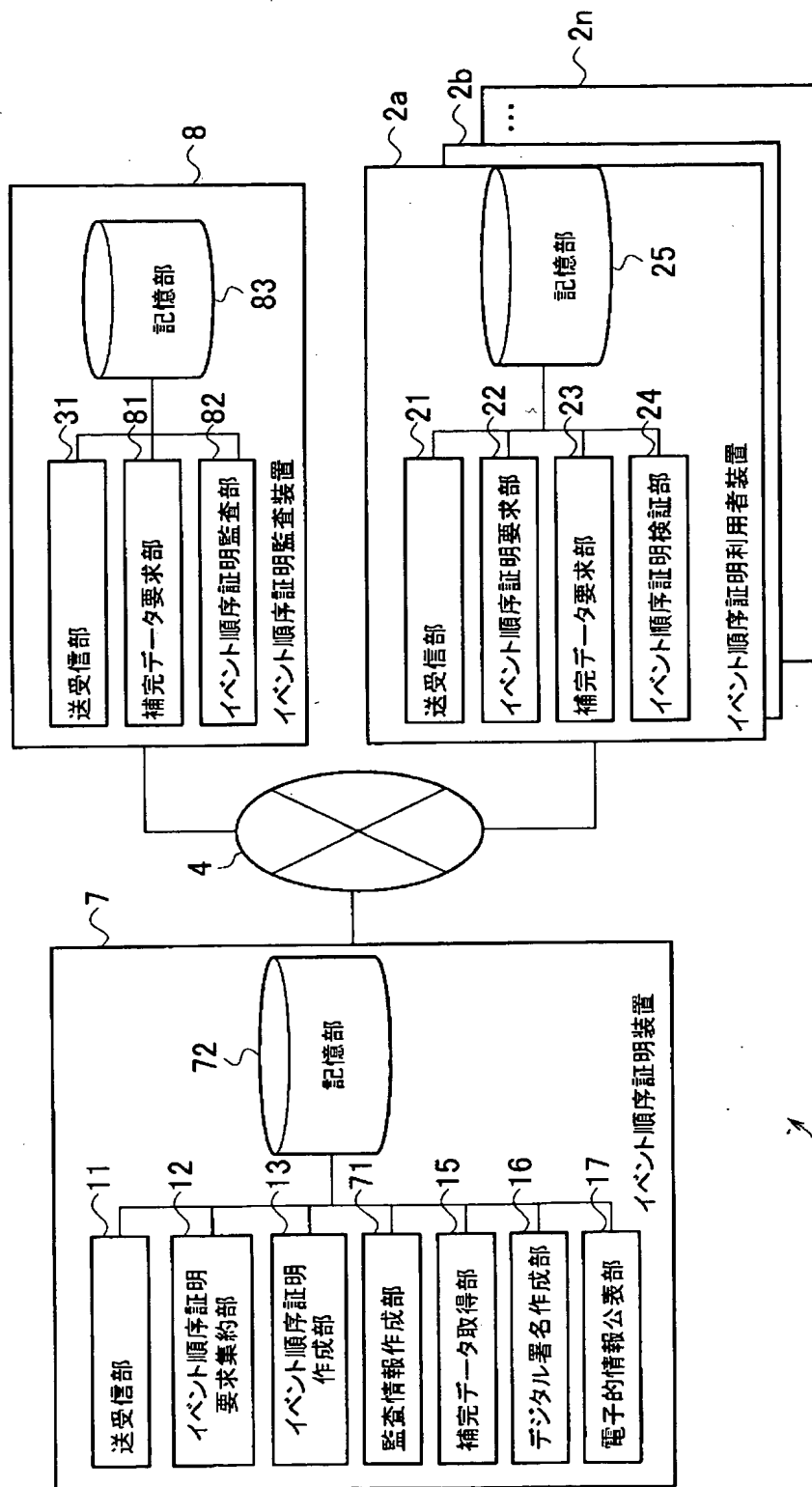


【図 9】



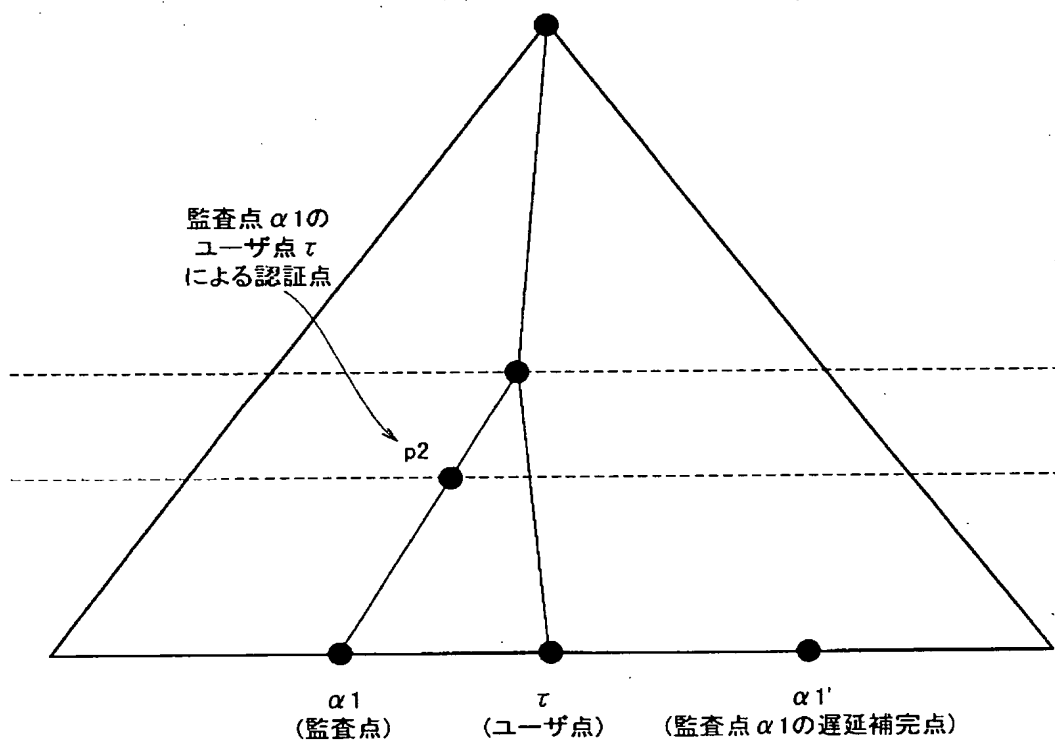
【図 10】

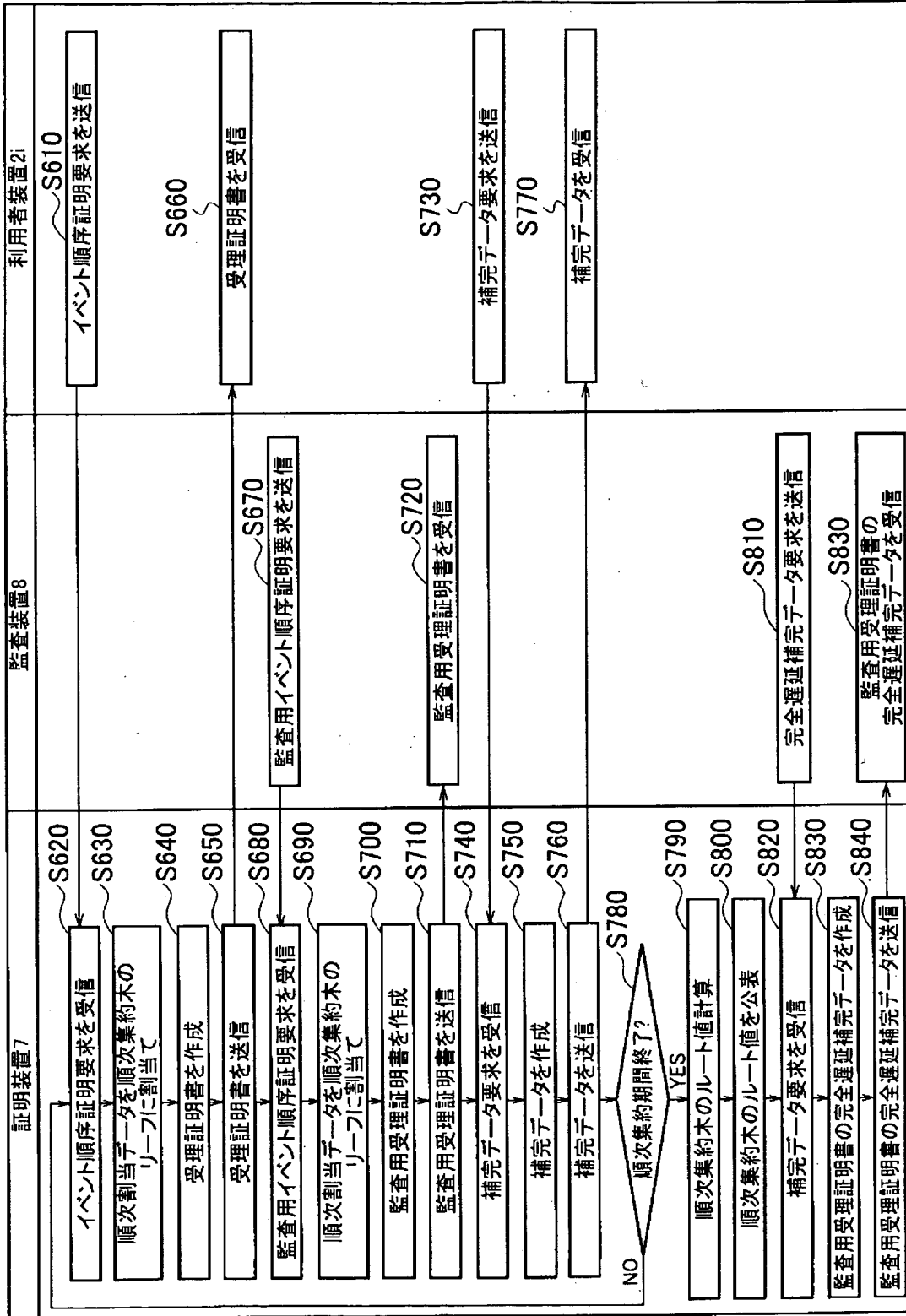


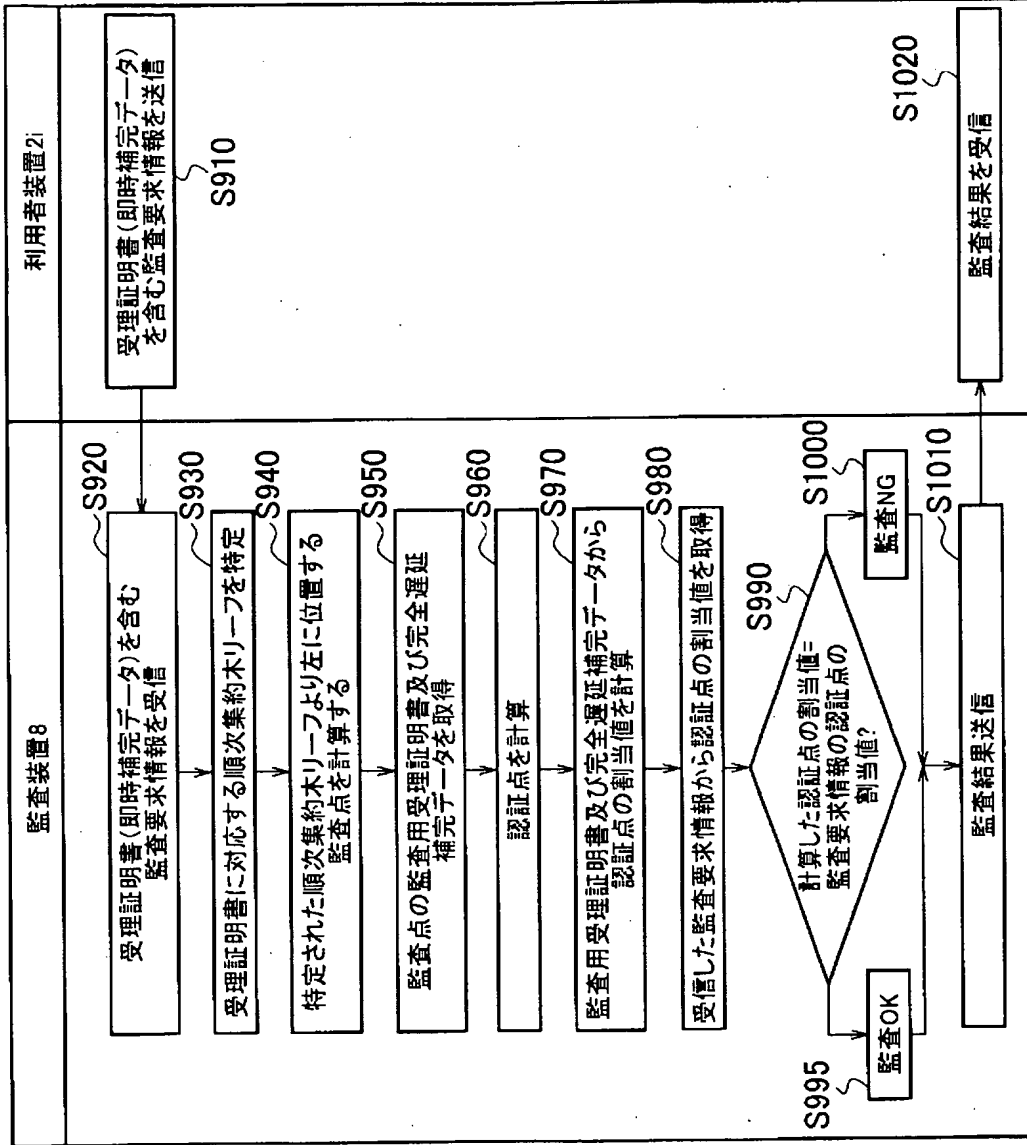


200 イベント順序証明システム

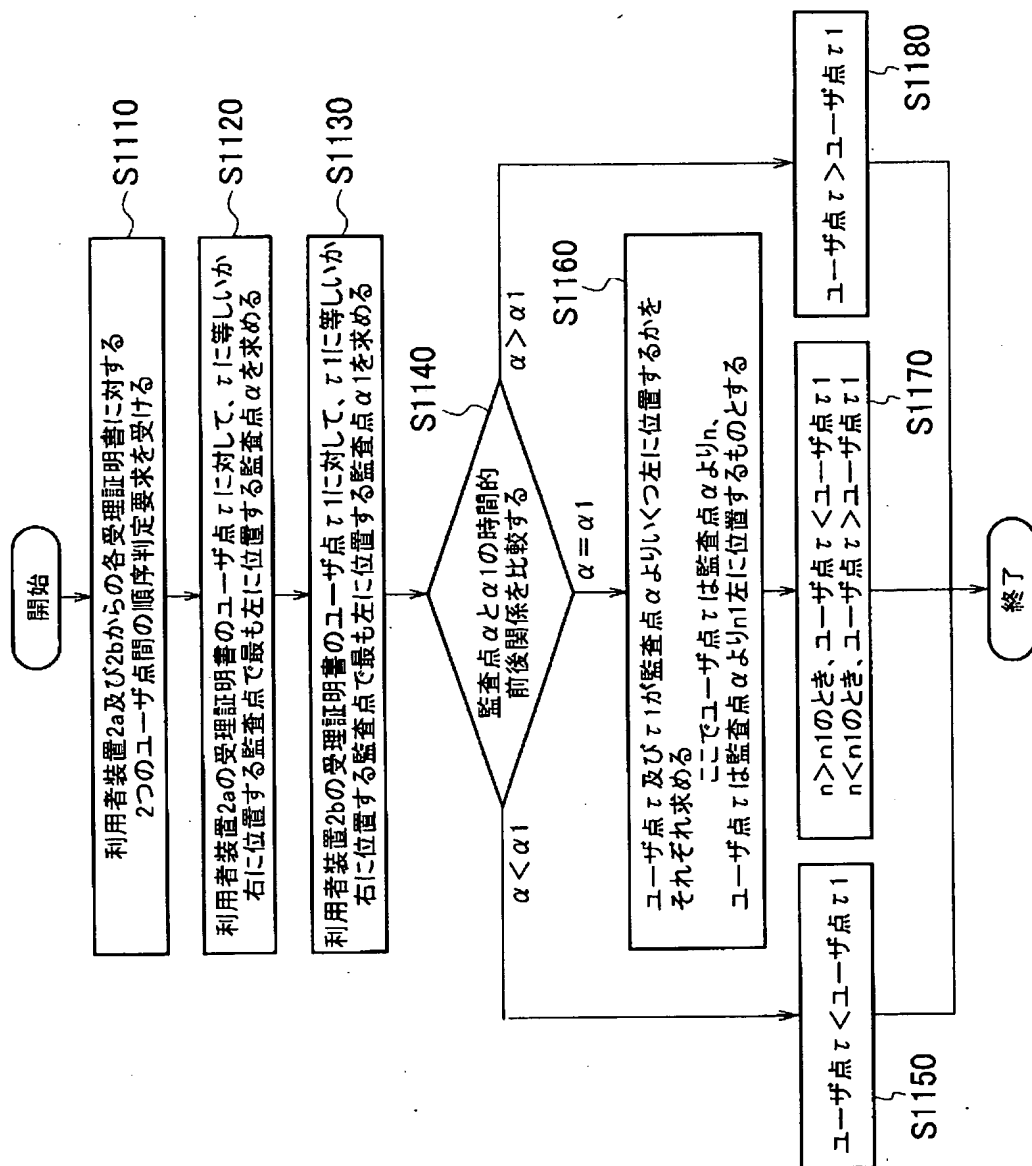
【図 1 2】



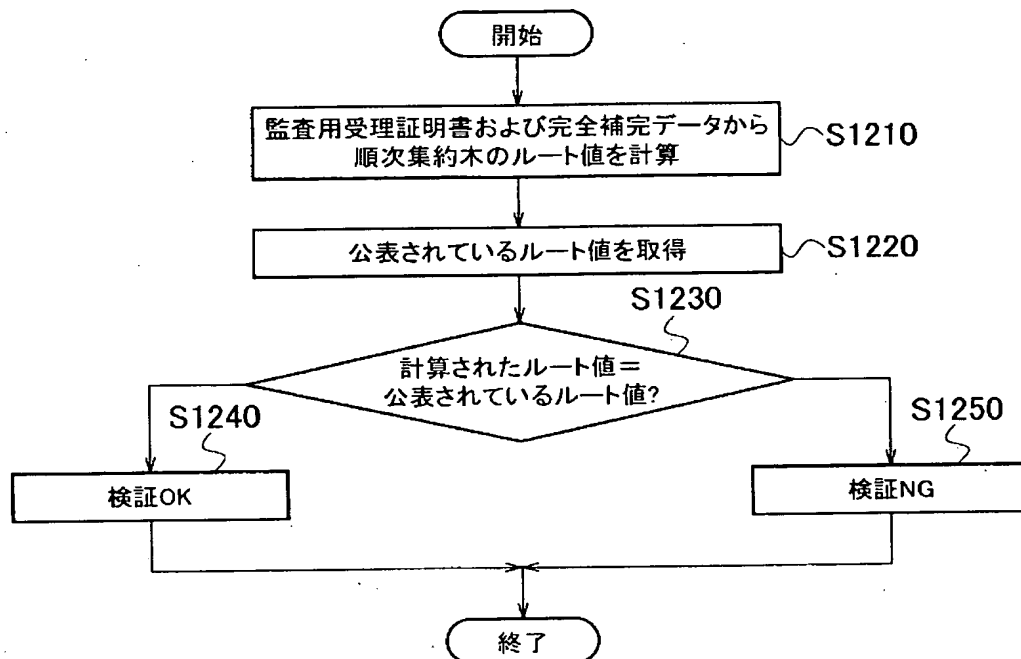




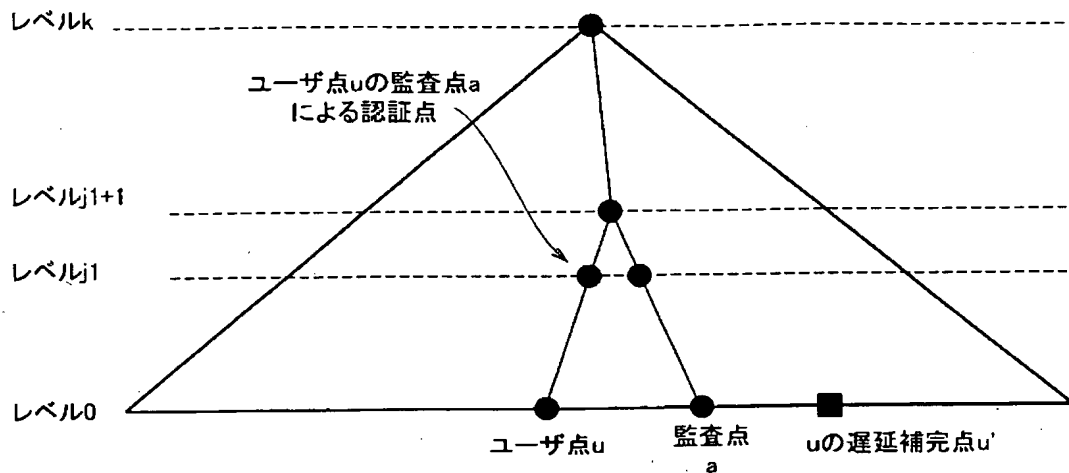




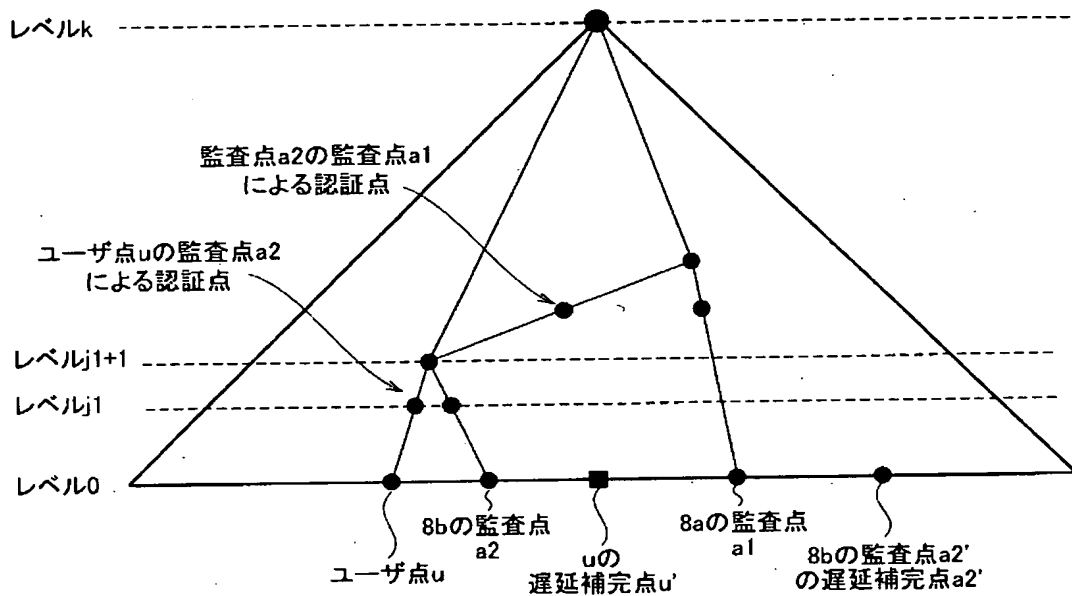
【図16】

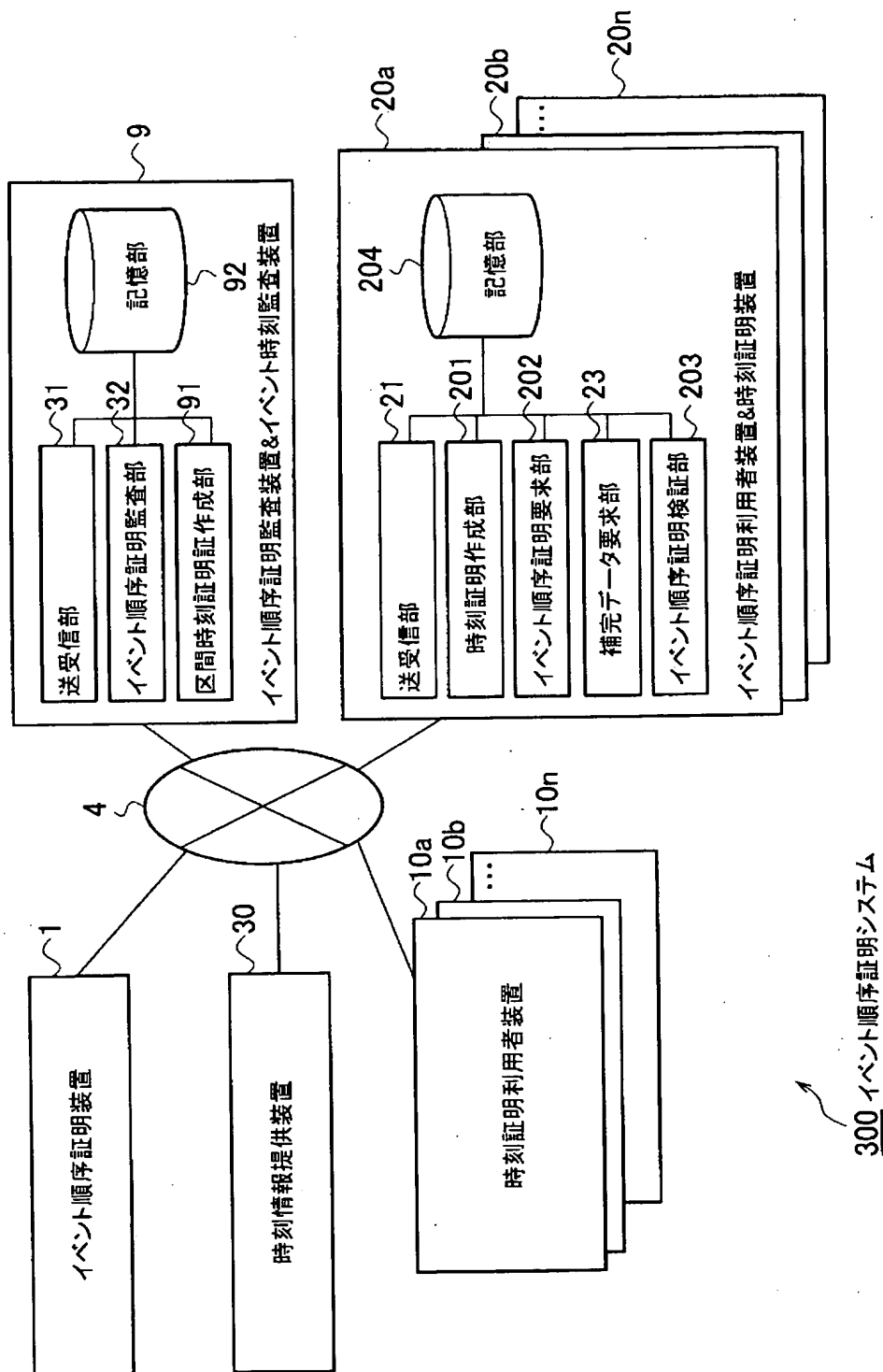


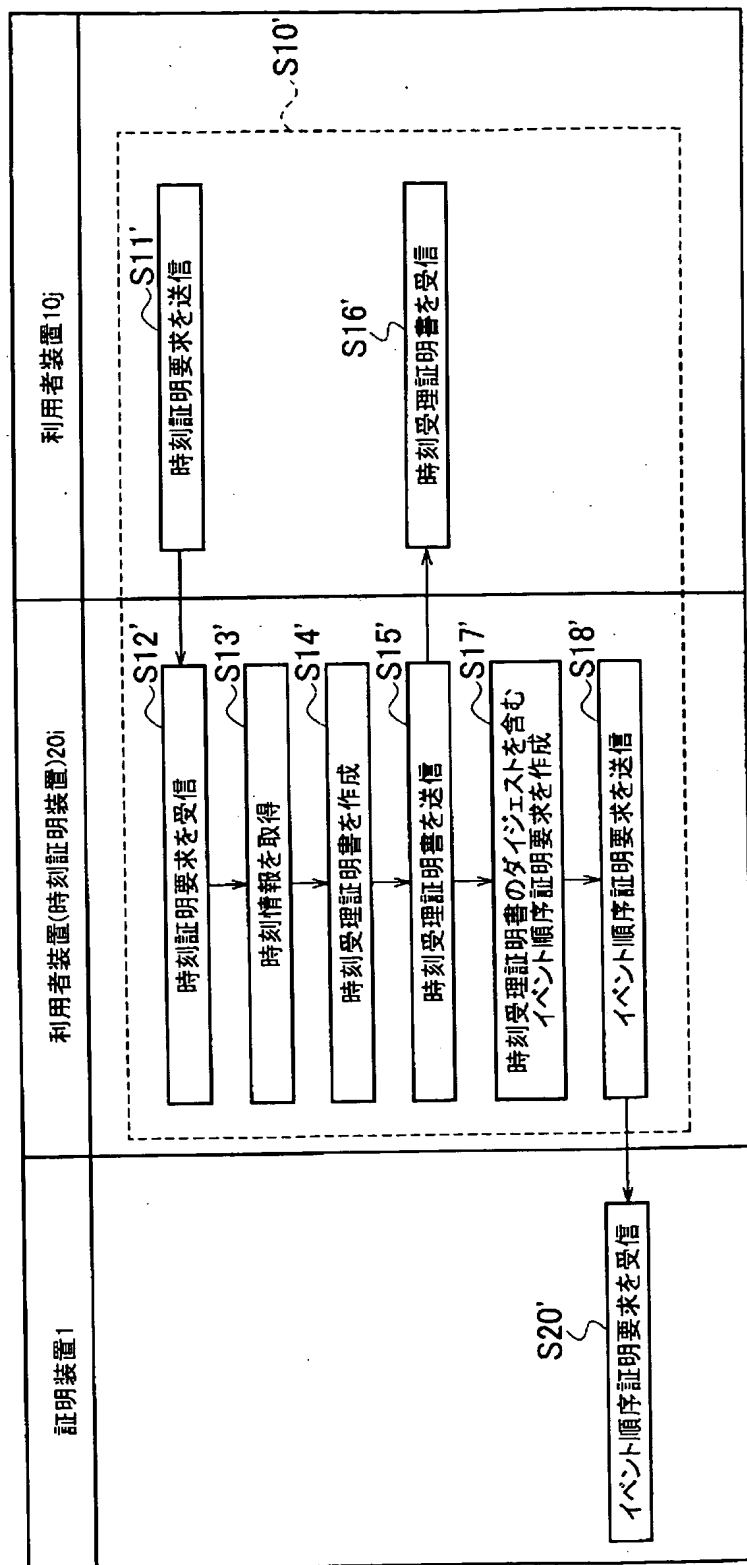
【図 17】



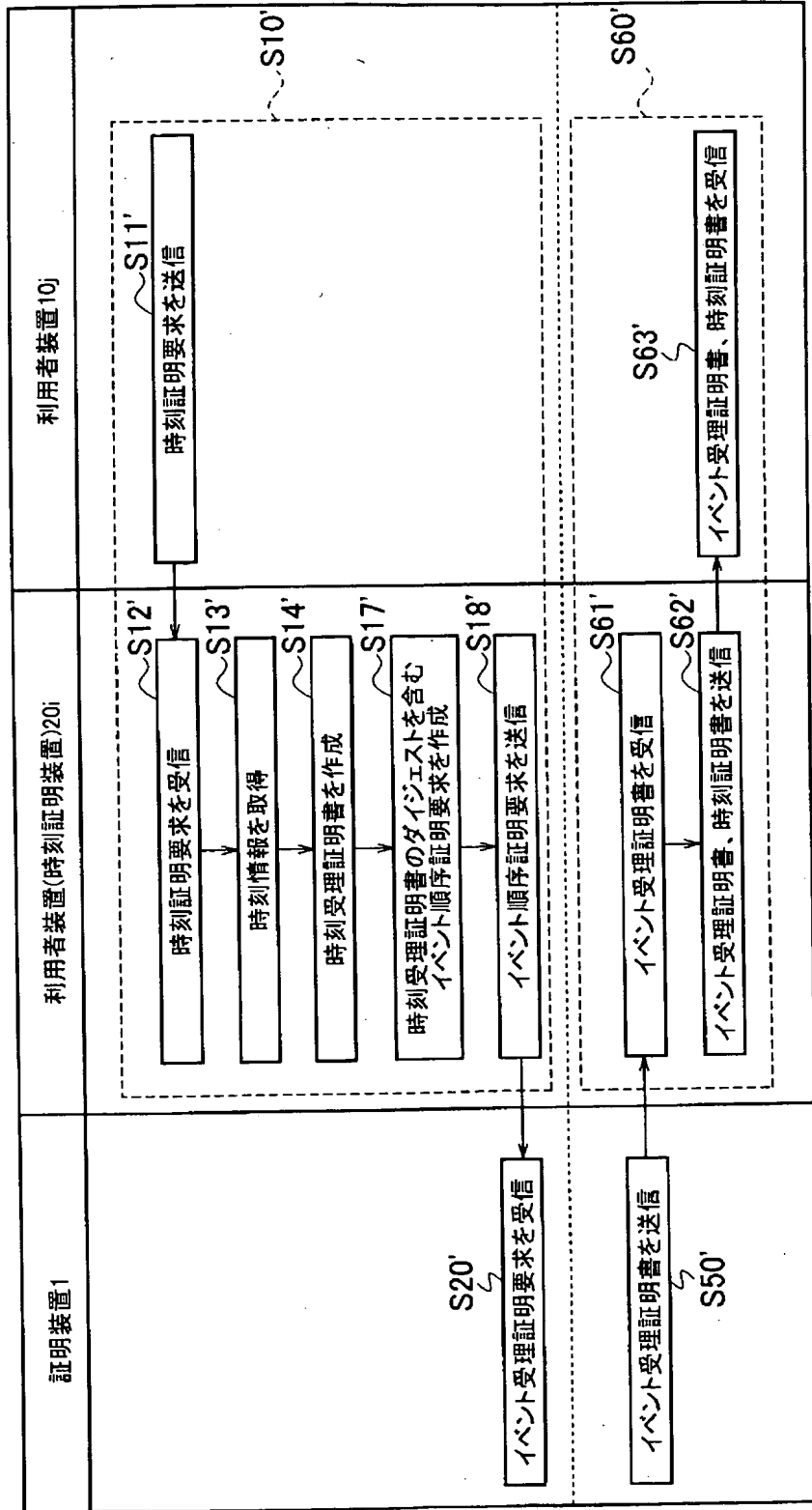
【図 18】



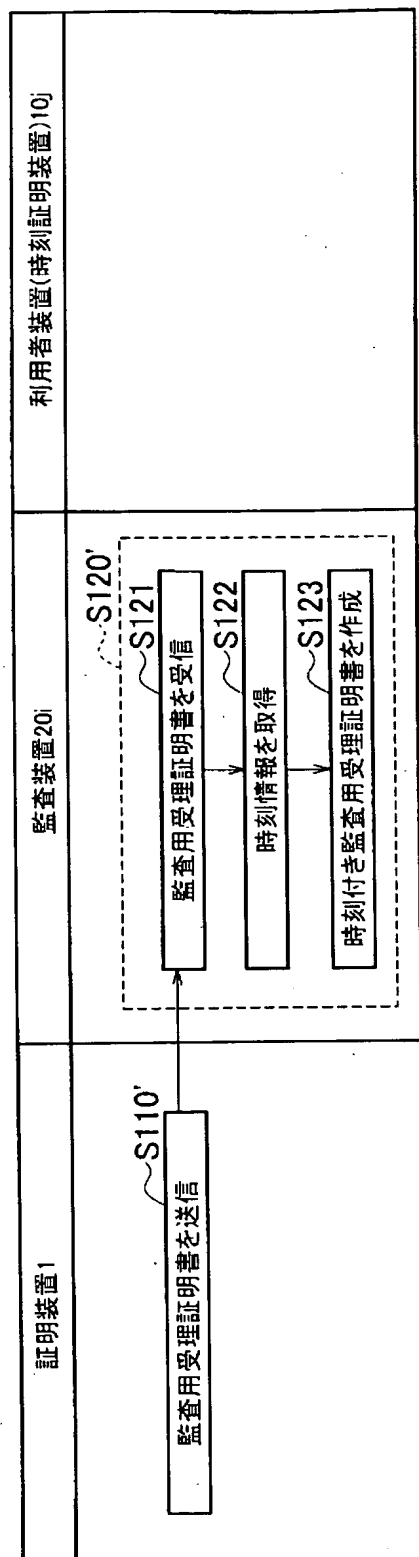


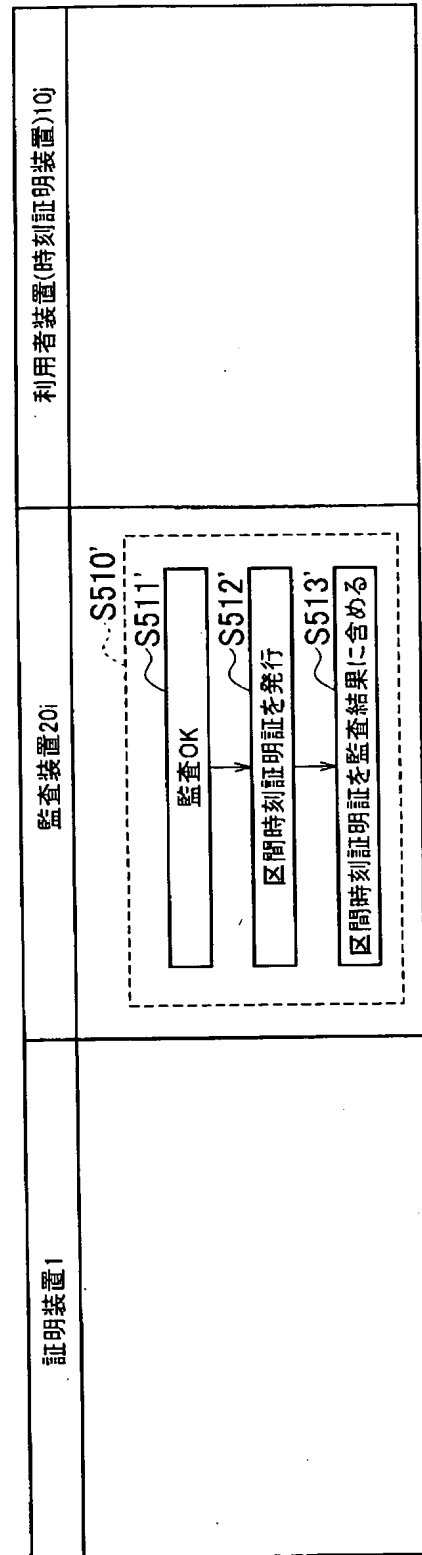


【図 2 1】

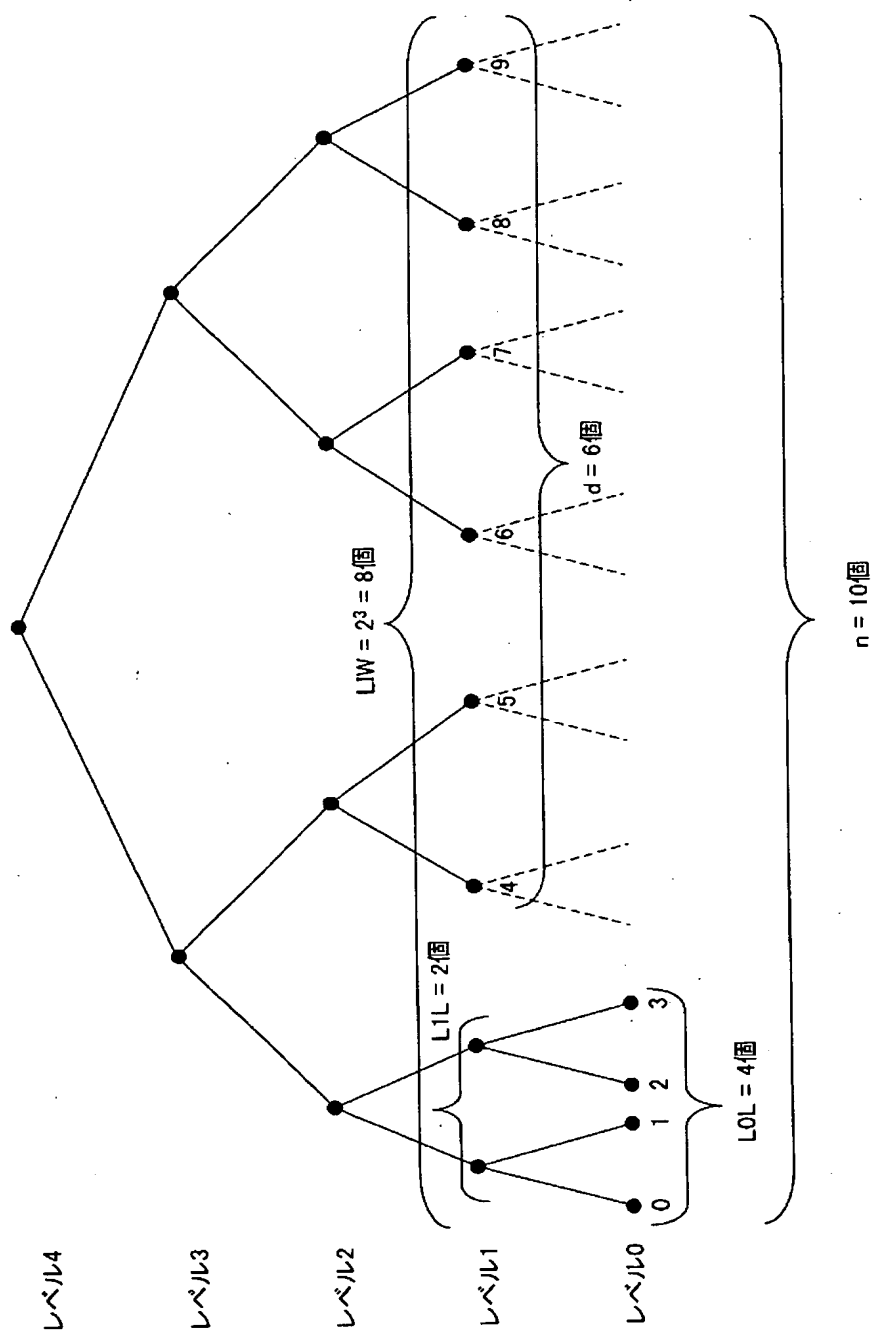


【図 2 2】









(1) ループ1 : 構成法その3では、定められた時間間隔が終了するまで以下の処理を繰り返す。

(1.1) 受け付けた要求を $x$ に置く。

(1.2)  $n$ を1インクリメントする。

(1.3) ループ2 :  $j = 0, \dots, K$ に対して以下の処理を行う。

(1.3.1)  $i := i_j$ と置く。

(1.3.2)  $j = 0$ のときは、 $A_j[i] := x$   
(即ち、ノード $(j, i)$ に $x$ を設定する)。

(1.3.3)  $j > 0$ のときは、以下を行う。

- $x0 := A_{j-1}[\text{index}(\text{leftChild}(j, i))]$   
(ノード $(j, i)$ のleft-childに割り付けられた値を $x0$ とおく)。

- $x1 := A_{j-1}[\text{index}(\text{rightChild}(j, i))]$   
(ノード $(j, i)$ のright-childに割り付けられた値を $x1$ とおく)。

- $x2 := h(x0 \parallel x1)$ を計算する。

- $A_j[i] := x2$   
(即ち、ノード $(j, i)$ に $x2$ を割り付ける)。

(1.3.4)  $i_j$ を1インクリメントする。

(1.3.5)  $i$ が偶数のときは、ループ2を抜ける。

ループ2終了。

ループ1終了。

処理手順1

(2) 終了時間がきて、ループ1を抜けた後では次の処理を行う。

(2.1)  $k := \text{ceiling}(\log_2(n))$  とおく。

(2.2)  $\text{rtPath}(k, 0, n-1)$  を計算し、その結果を  $((0, r(0)), \dots, (k, r(k)))$  と置く。

(2.3) ループ3:  $j = 0, \dots, k$  に対して以下の処理を行う。

(2.3.1)  $i = i_j$  とおく。

(2.3.2)  $j = 0$  のとき:

(2.3.2.1)  $i$  が奇数のとき:

- ・ダミー値  $r := R(0, i)$  を生成する。
- ・ $A_j[i] := r$   
(ノード  $(0, i)$  に  $r$  を割り当て)。
- ・ $b_j := \text{true}$  と置く。
- ・ $i_j$  を1インクリメントする。

(2.3.2)  $0 < j \leq k$  のとき:

(2.3.2.1)  $i = r(j)$  のとき:

(即ち、ノード  $(j, i)$  が  $\text{rtPath}(k, 0, n-1)$  上にあるとき):

(2.3.2.1.1)  $x0 := A_{j-1}[\text{index}(\text{leftChild}(j, i))]$

(ノード  $(j, i)$  の left-child に割り付けられた値を  $x0$  と置く)。

(2.3.2.1.2)  $x1 := A_{j-1}[\text{index}(\text{rightChild}(j, i))]$

(ノード  $(j, i)$  の right-child に割り付けられた値を  $x1$  と置く)。

(2.3.2.1.3)  $x2 := h(x0 \parallel x1)$  を計算する

(2.3.2.1.4)  $A[j] := x2$

(即ち、ノード  $(j, i)$  に  $x2$  を割り付ける)。

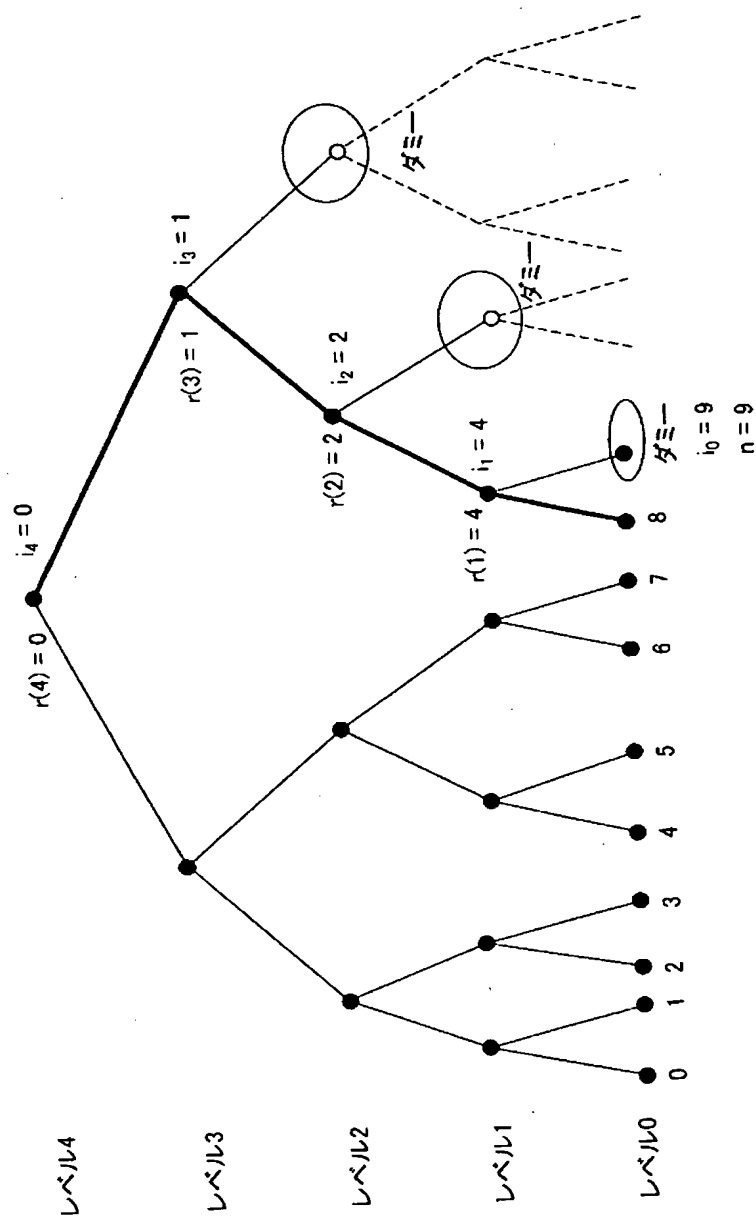
(2.3.2.1.5)  $i$  が偶数で  $j < k$  のとき:

- ・ $i$  を1インクリメントする。
- ・ $r := R(j, i)$  を計算し、 $A_j[i] := r$   
(即ち、ノード  $(j, i)$  に  $r$  を割り当てる)。
- ・ $b_j := \text{true}$  と置く。
- ・ $i_j := i+1$  と置く。

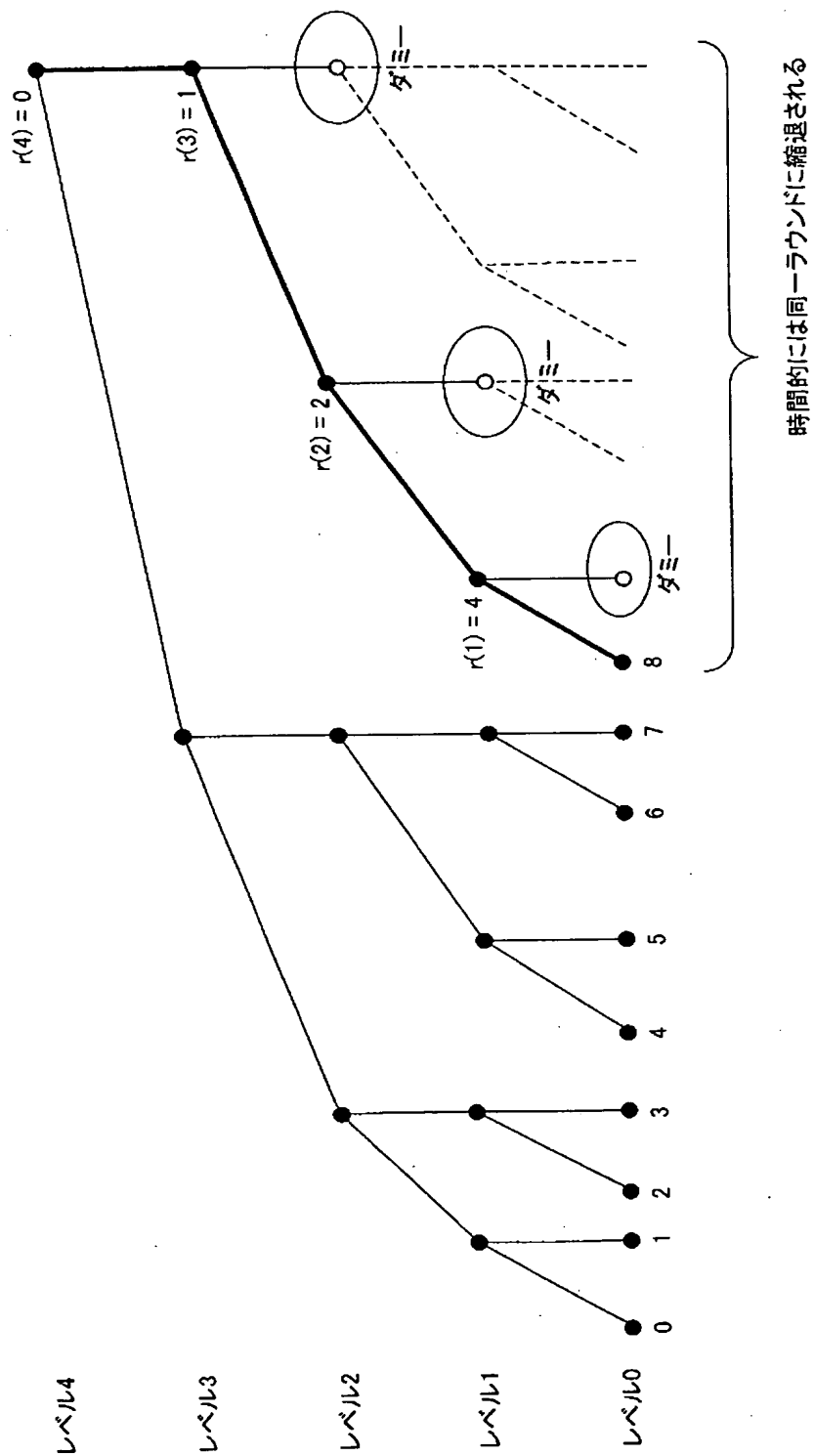
(2.3.2.2)  $i = r(j)+1$  で  $i$  が奇数で  $j < k$  のとき:

- ・ $r := R(j, i)$  を計算し、 $A_j[i] := r$   
(即ち、ノード  $(j, i)$  に  $r$  を割り当てる)。
- ・ $b_j := \text{true}$  と置く。
- ・ $i_j$  を1インクリメントする。

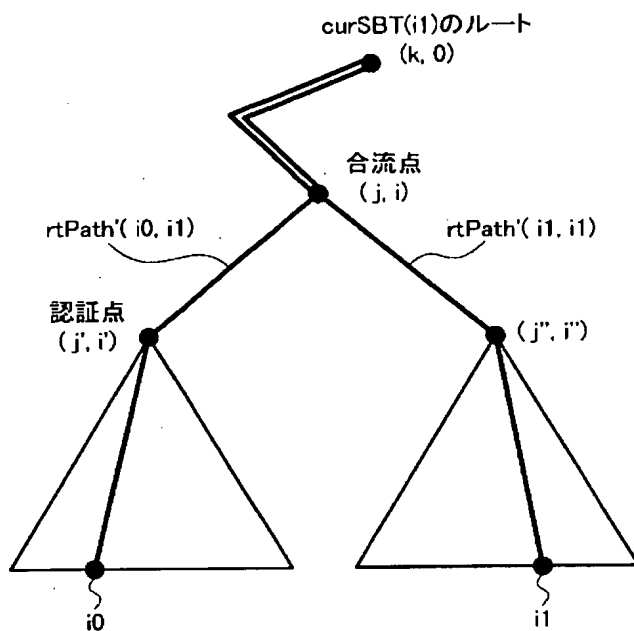
ループ3終了。



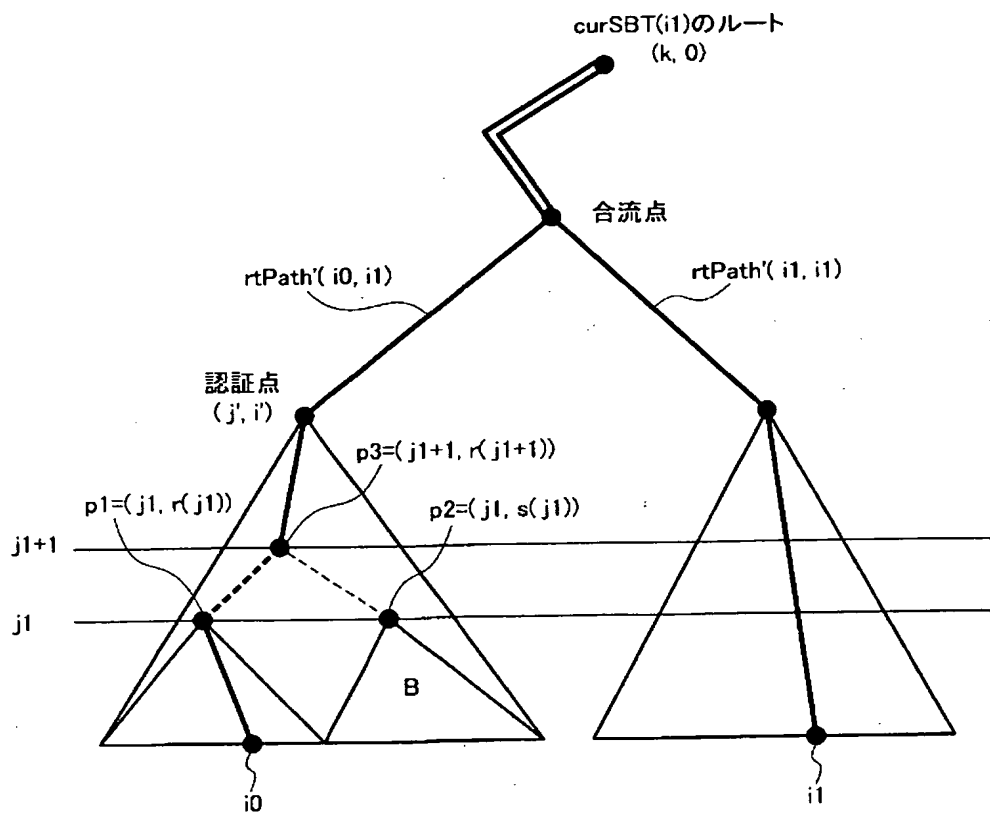
【図 2 8】



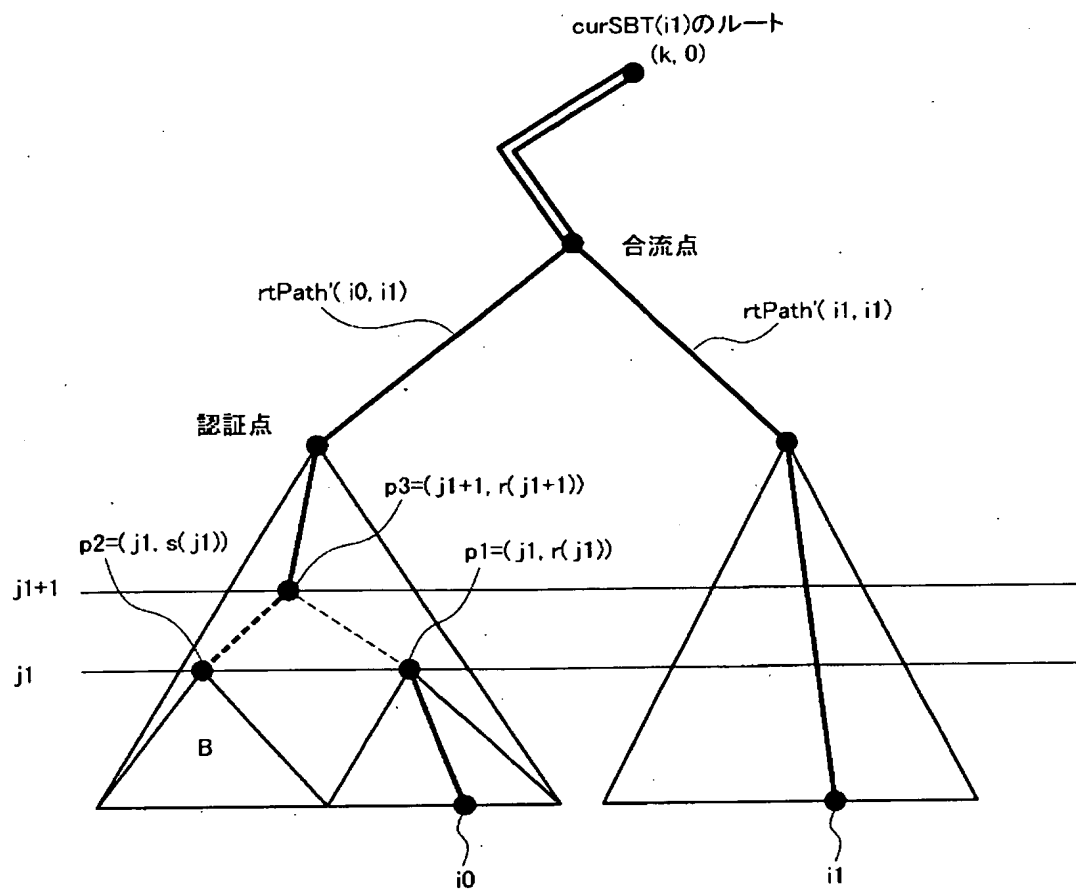
【図 29】



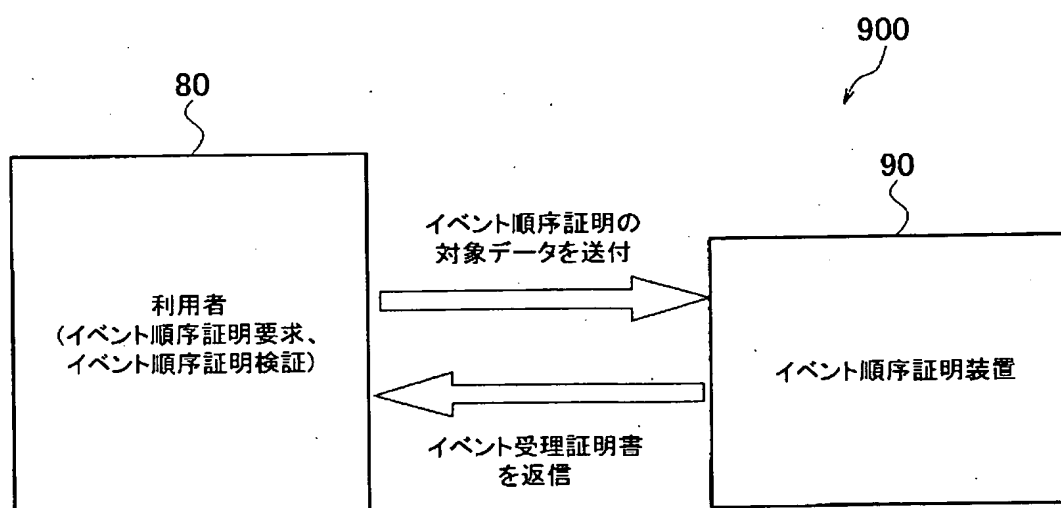
【図 30】



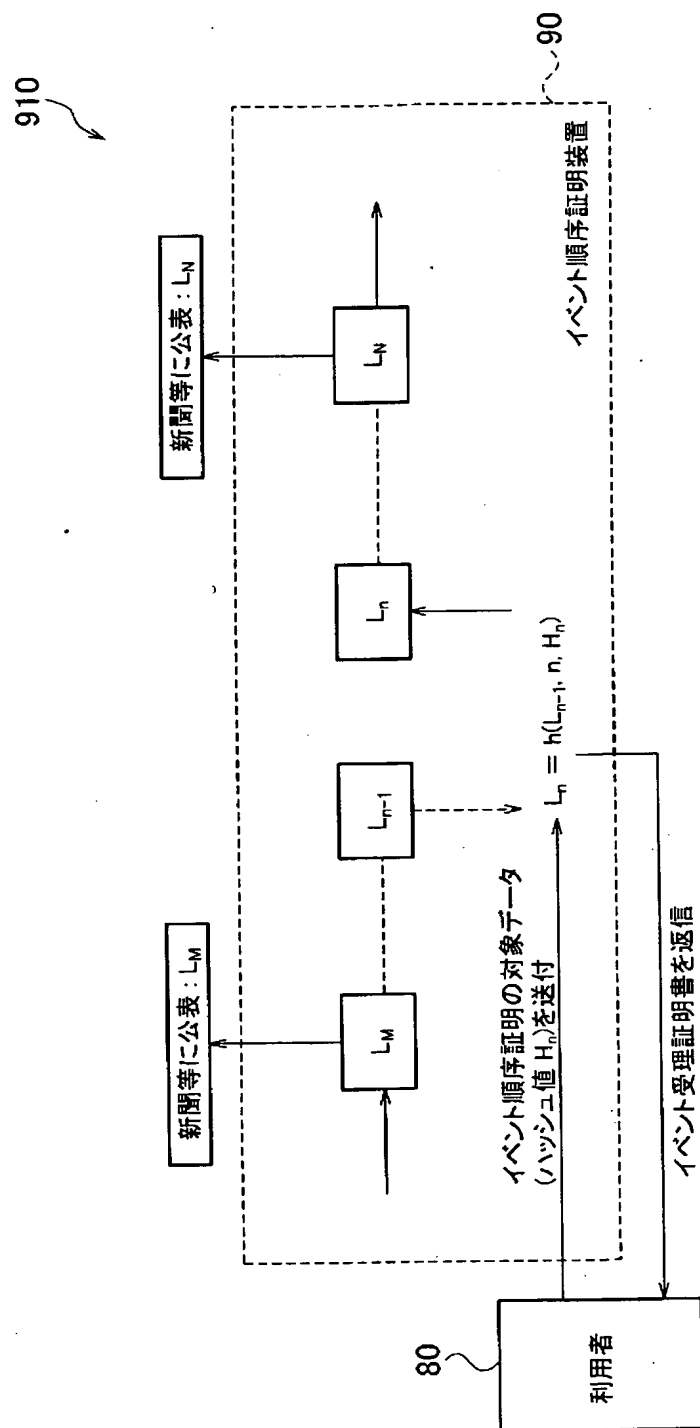
【図 3 1】



【図 3 2】



【図 3 3】





【書類名】要約書

【要約】

【課題】木構造を用いてイベント順序を証明するイベント順序証明システムにおいて、イベント順序証明要求をまとめた公表データを用いなくても、イベント順序証明機関から発行されたイベント順序受理証明書の検証を行うことができる。

【解決手段】イベント順序証明システム100は、証明装置1、複数の利用者装置2i ( $i=a, b, \dots, n$ )、証明装置1が発行したイベント順序受理証明書の監査を行う監査装置3、及び、以上の各装置を相互に接続するコンピュータネットワーク4を備えており、証明装置1が利用者装置2iからのイベント順序証明要求に応じて、イベント順序受理証明書を発行し、利用者装置2iに返信すると共に、イベント順序受理証明書に疑義が生じた場合には、利用者装置2iは、証明装置1が公表したデータ又は監査装置3による監査結果によってイベント順序受理証明書を検証する。

【選択図】図1

出願人履歴

0 0 0 0 0 4 2 2 6

19990715

住所変更

5 9 1 0 2 9 2 8 6

東京都千代田区大手町二丁目3番1号

日本電信電話株式会社

FIG. 1

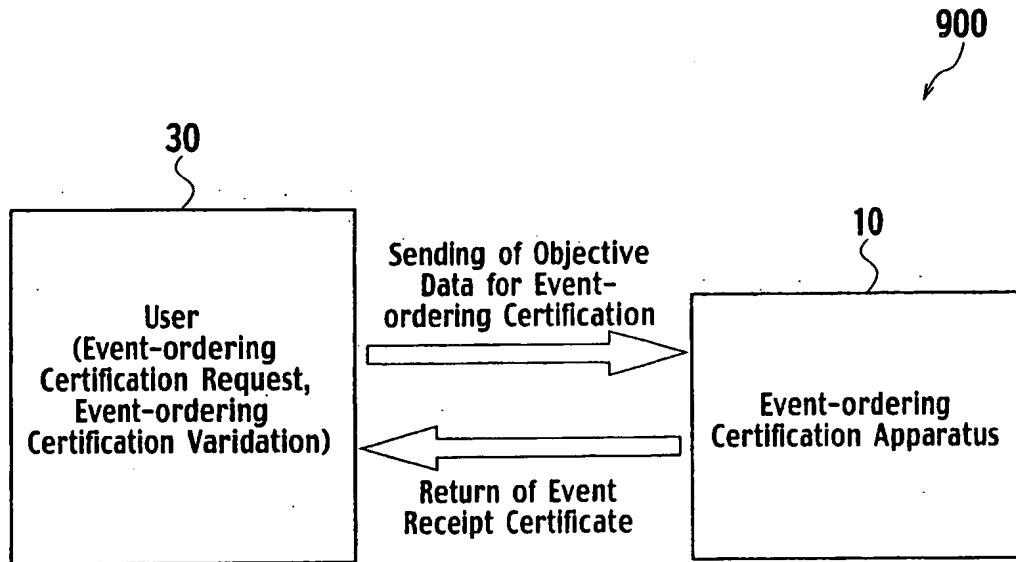


FIG. 2

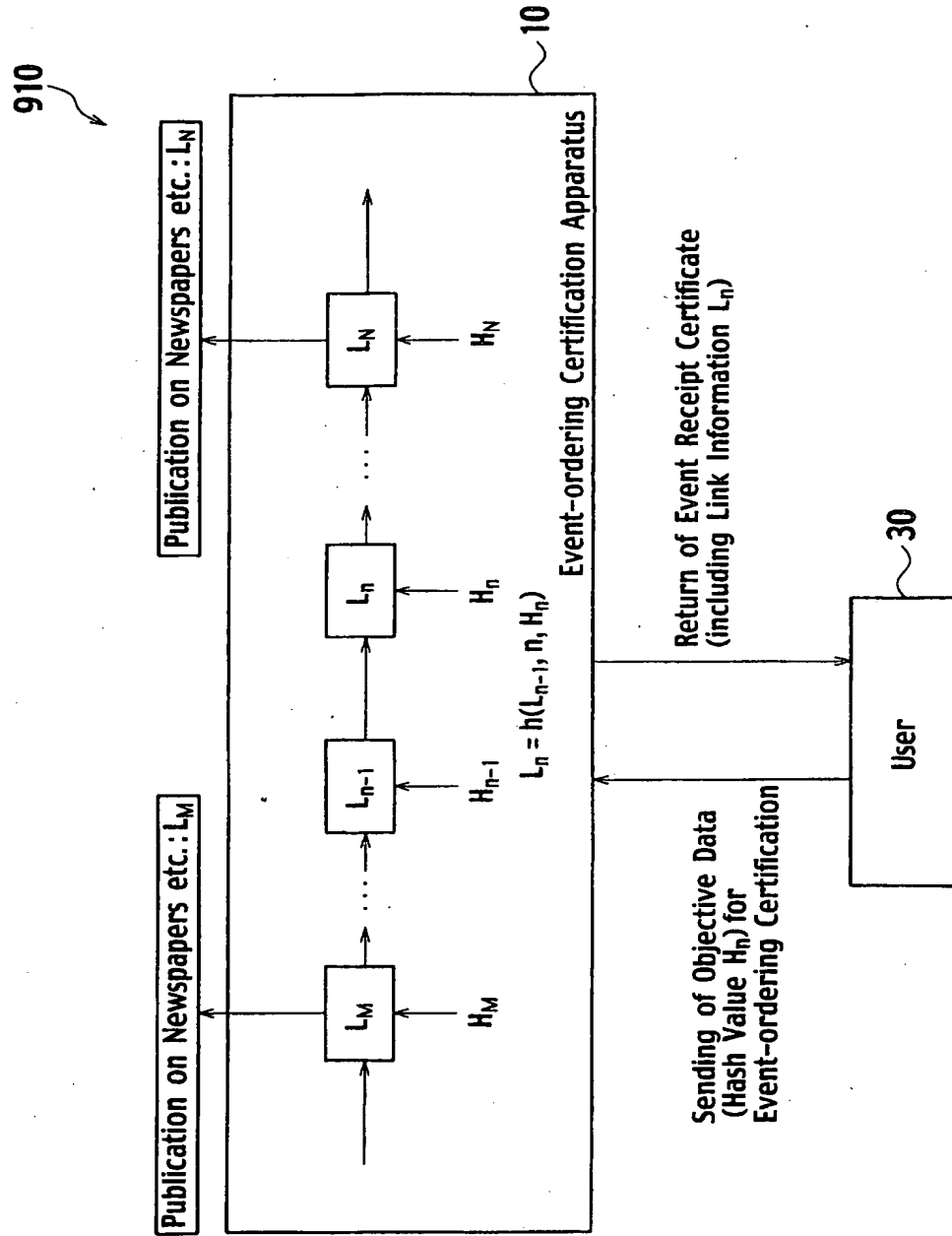


FIG. 3

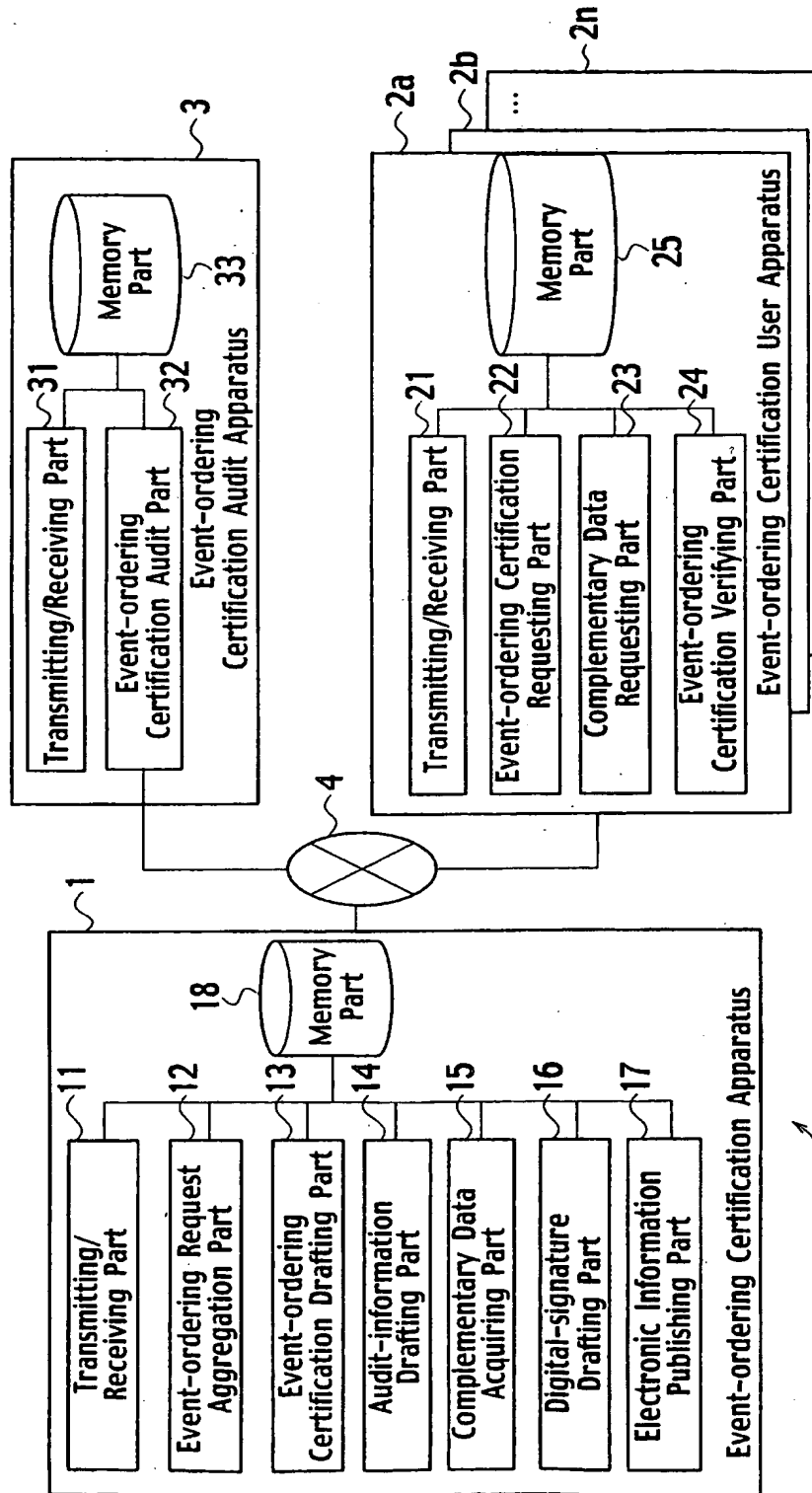


FIG. 4

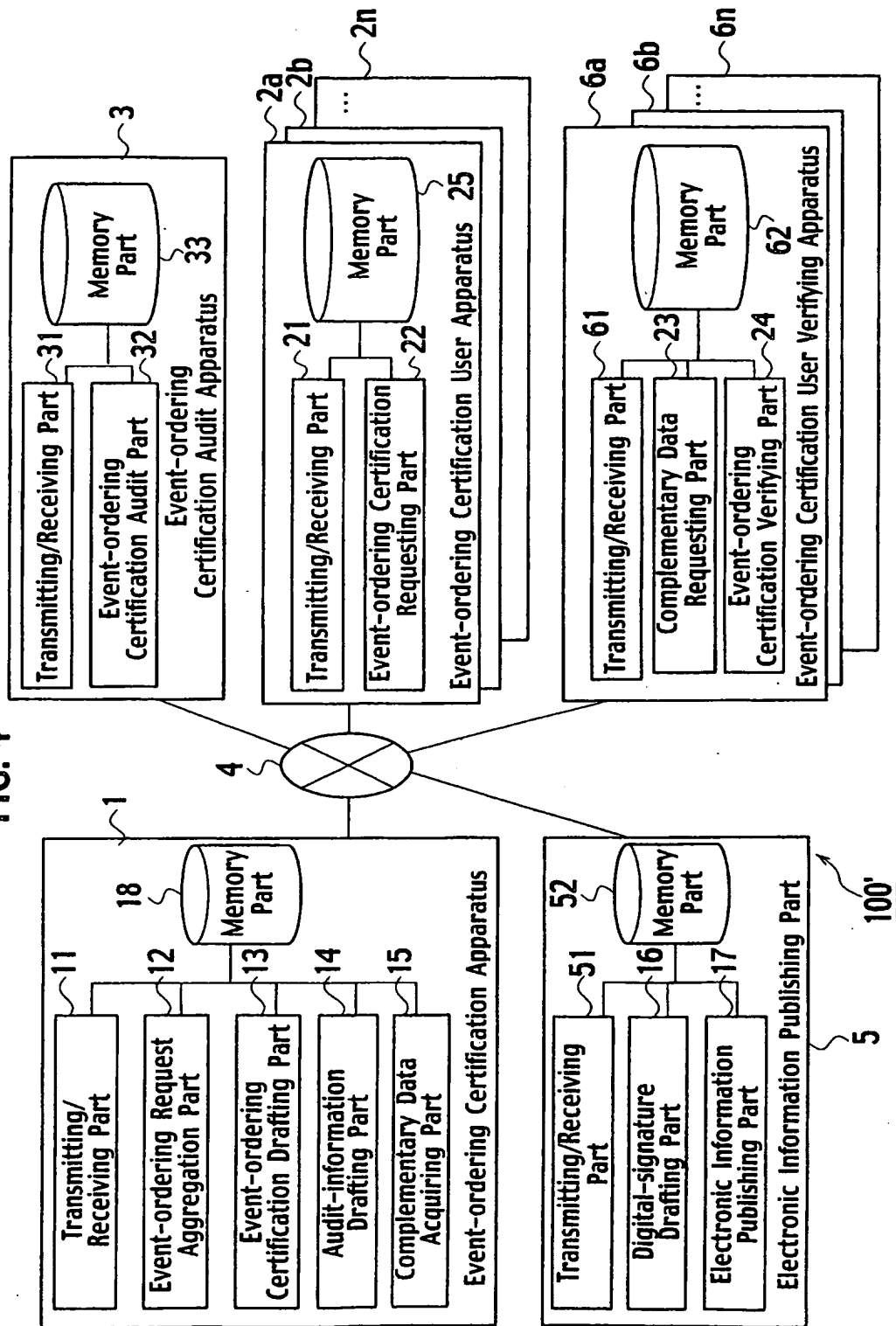
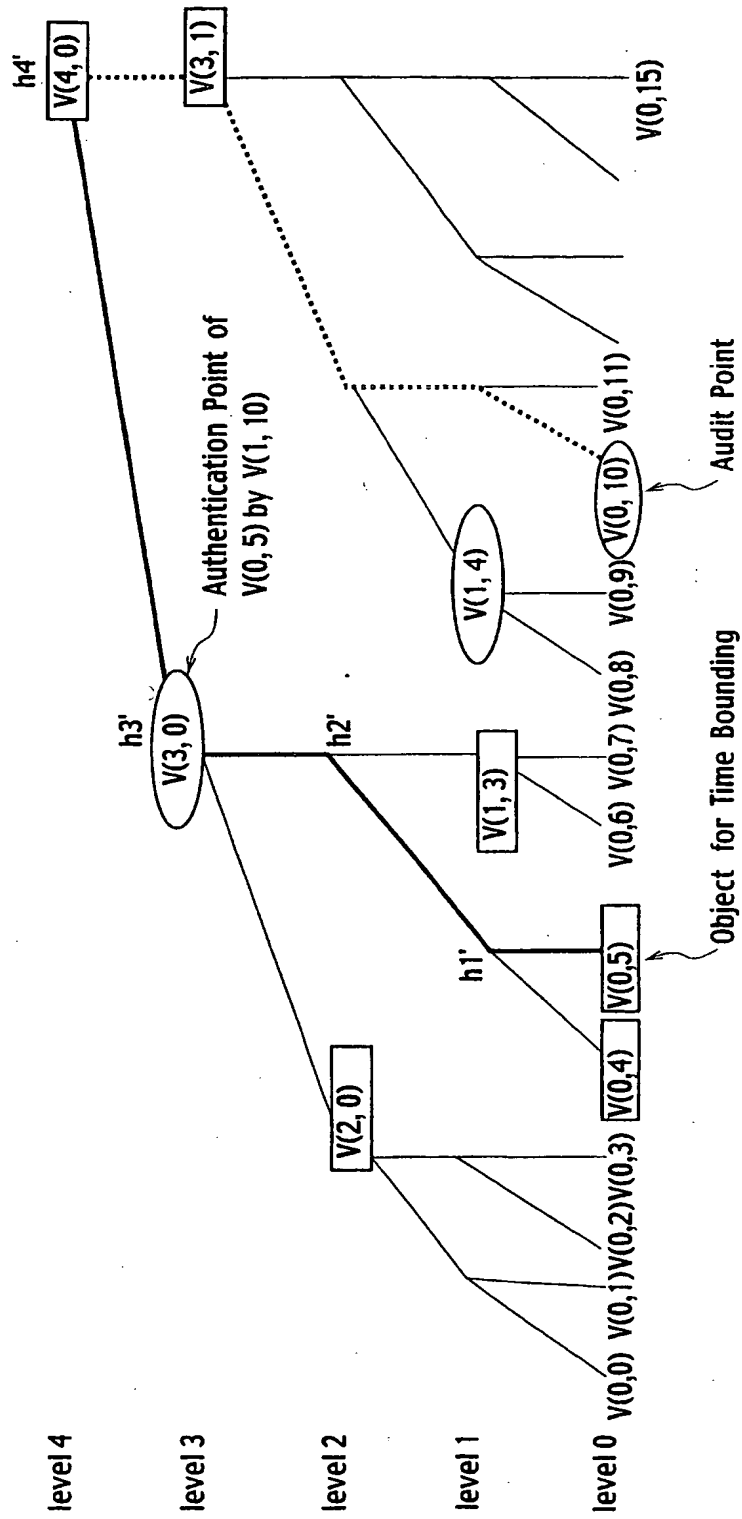


FIG. 5



**FIG. 6**

ITEM	SIGN	REQUIRED
Original Data	y	<input type="radio"/>
Sequentially Assigned Data-item	z	<input type="radio"/>
Sequential Aggregation Tree No.	n	<input type="radio"/>
Sequential Aggregation Tree Leaf No.	i	<input type="radio"/>
Immediate Complementary Data (Positional Info. Assigned Value)	HK	
Digital Signature	DS	



FIG. 7

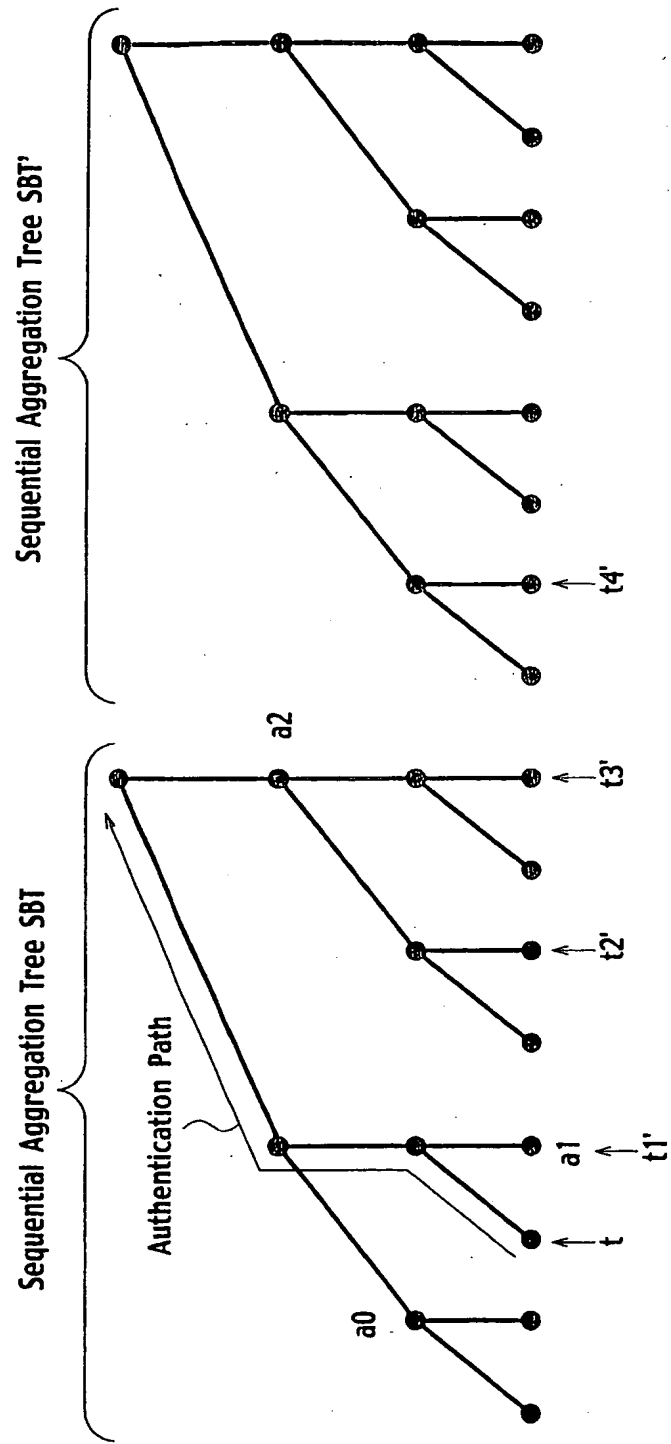


FIG. 8

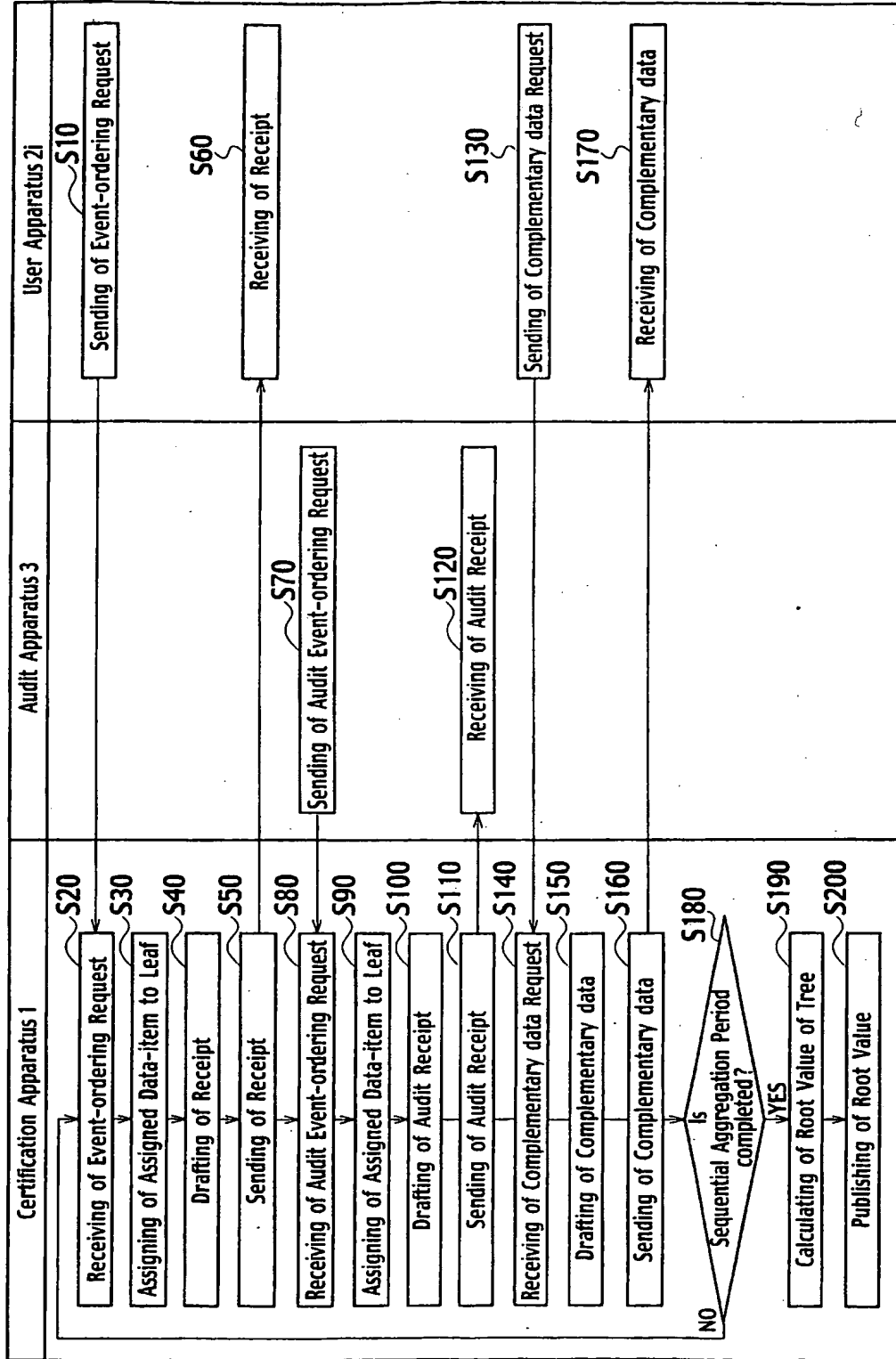


FIG. 9

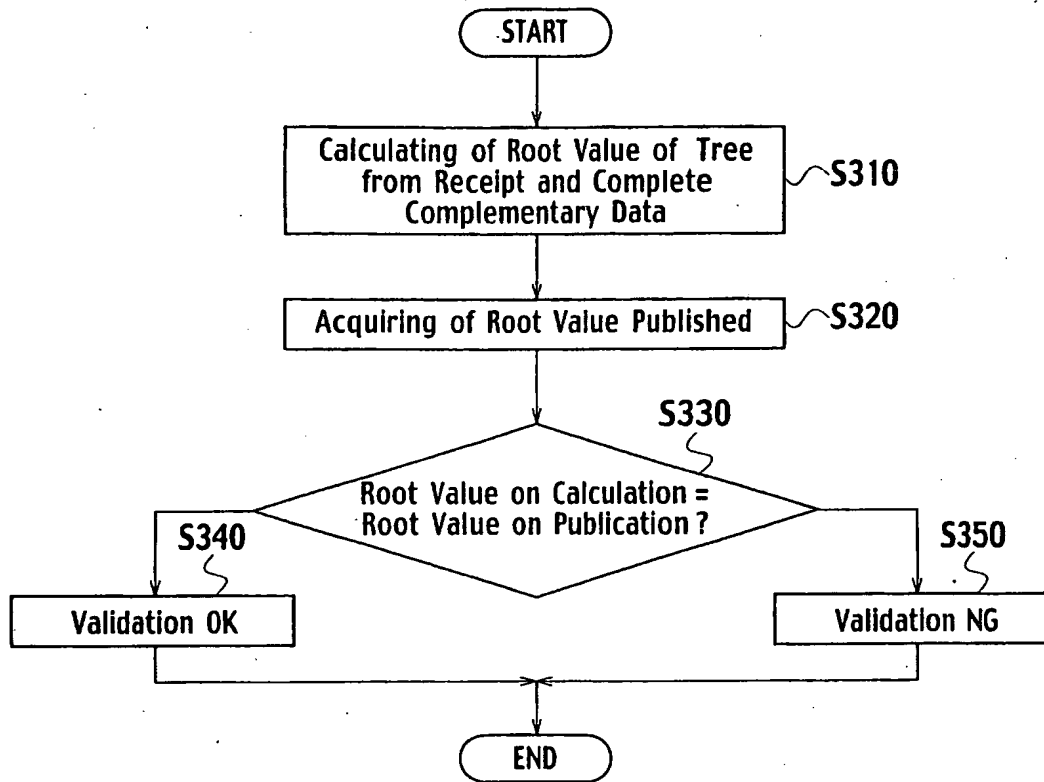


FIG. 10

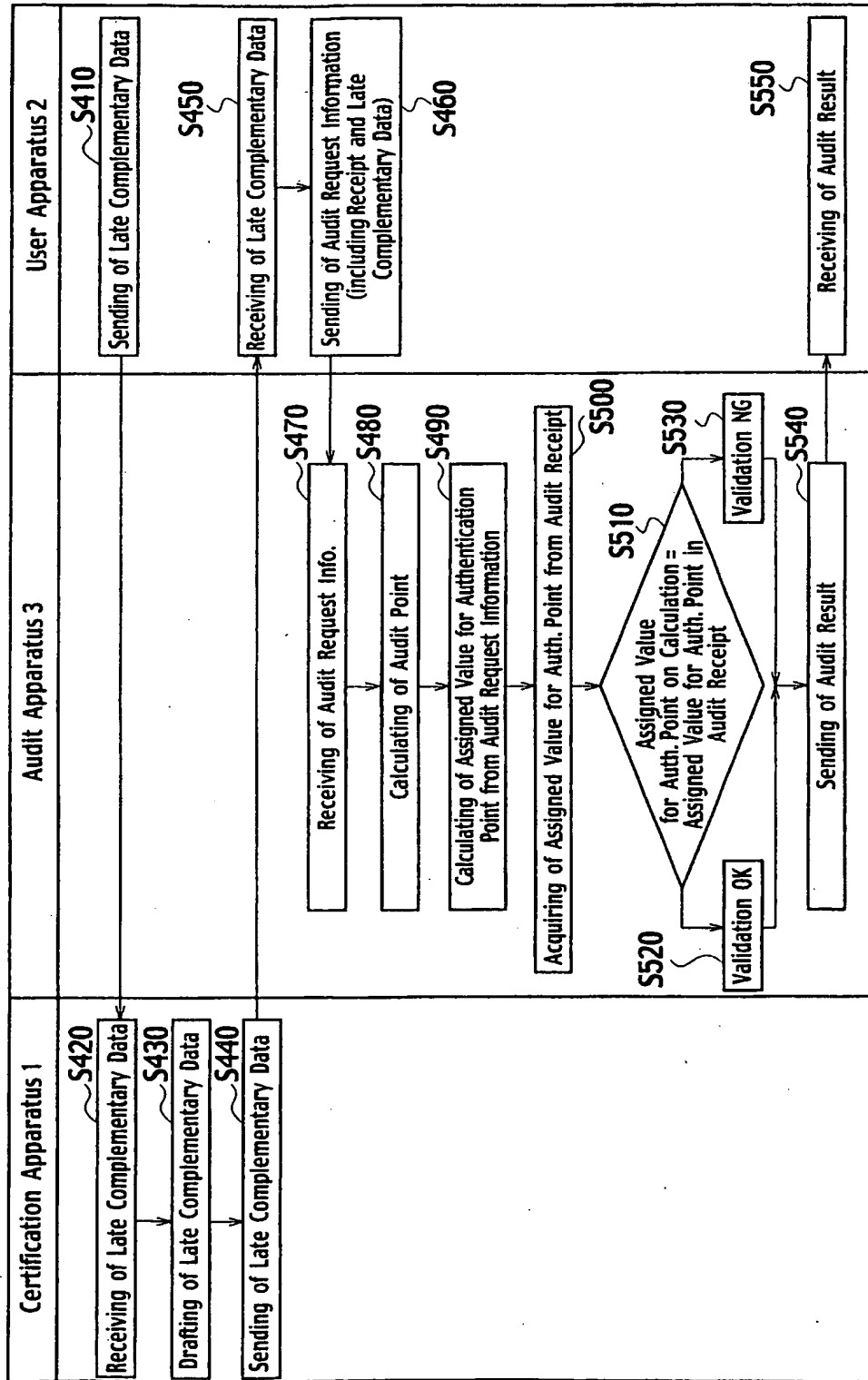


FIG. 11

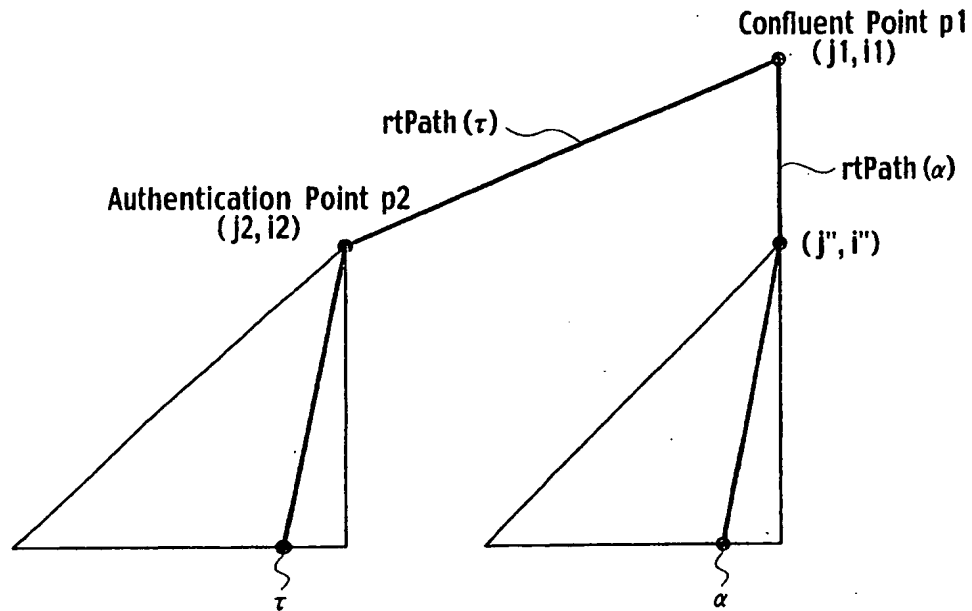


FIG. 12

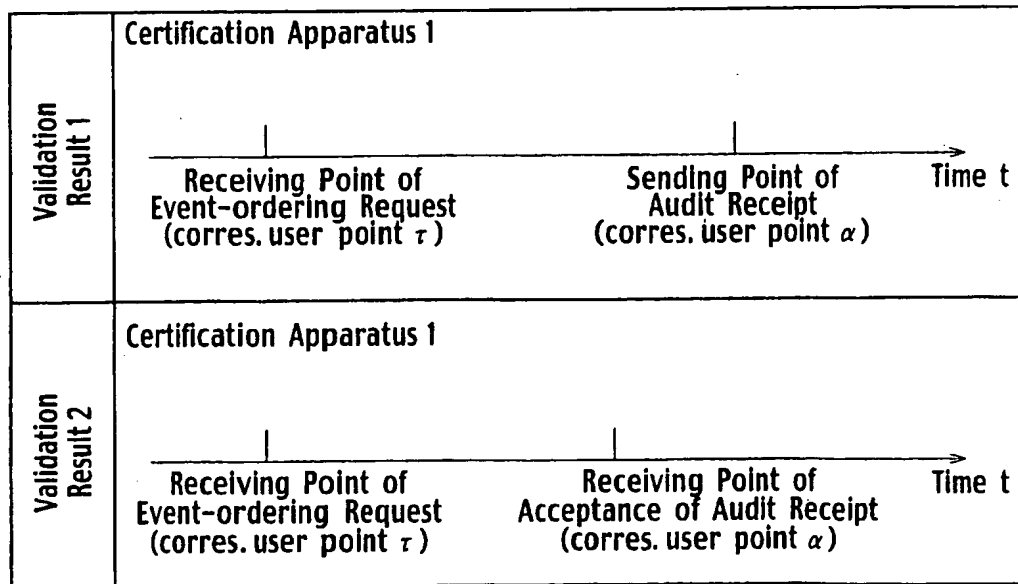


FIG. 13

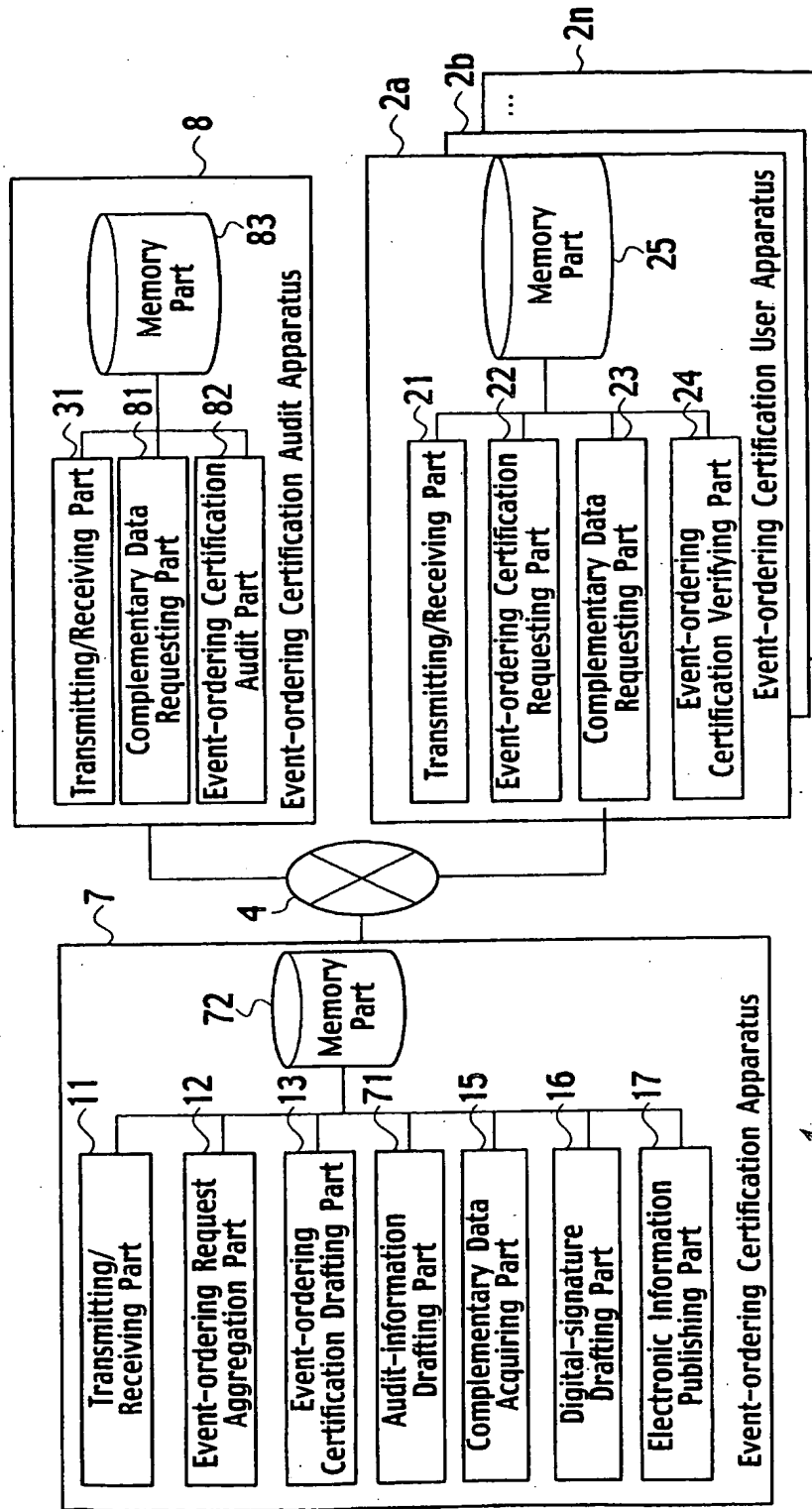


FIG. 14

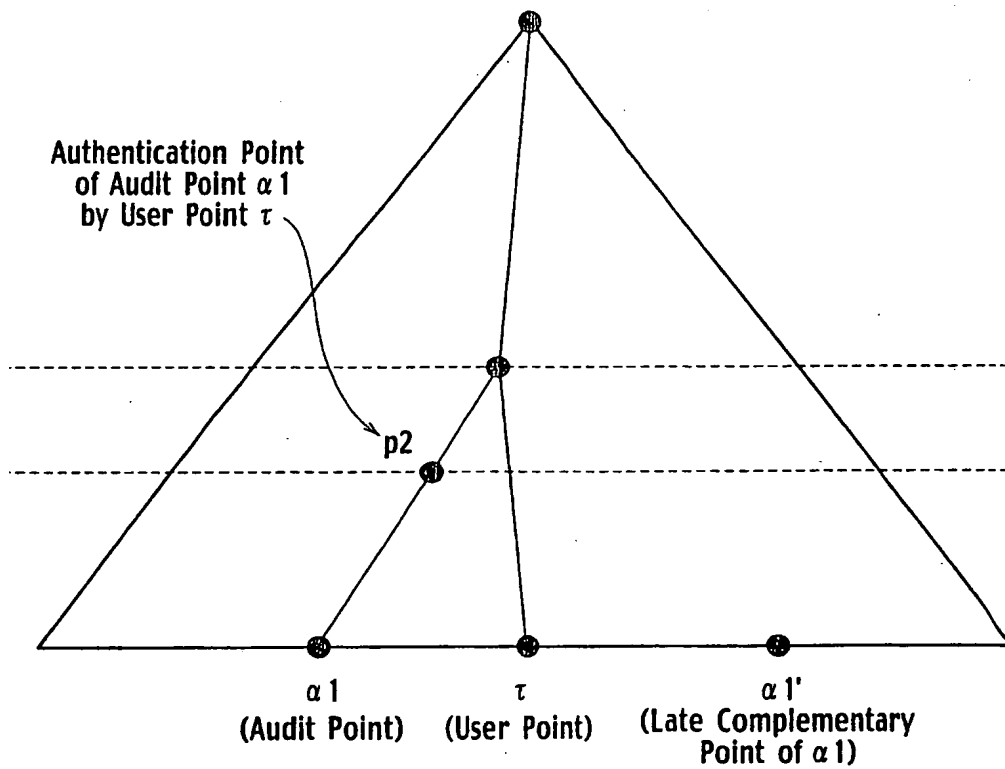


FIG. 15

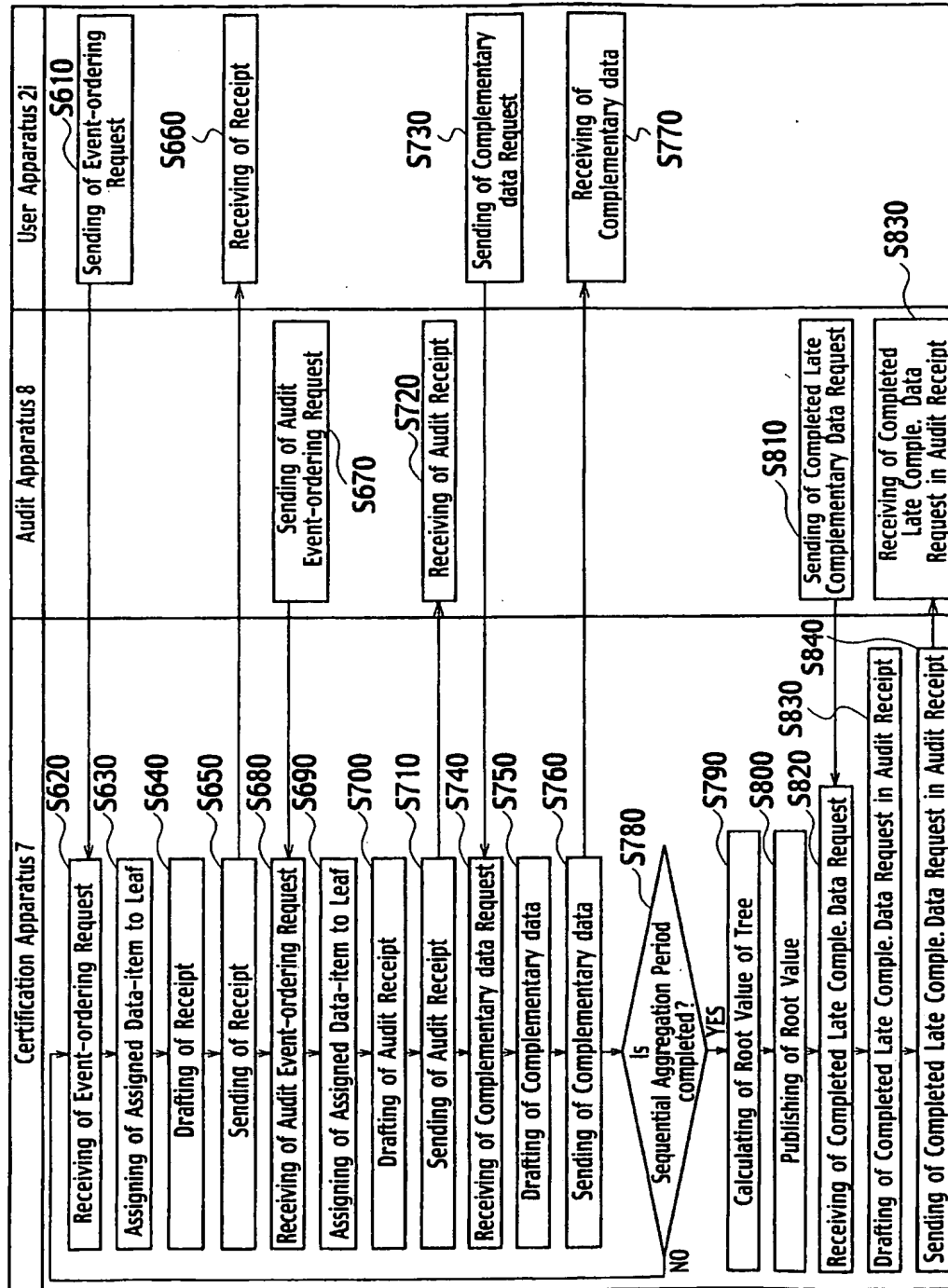




FIG. 16

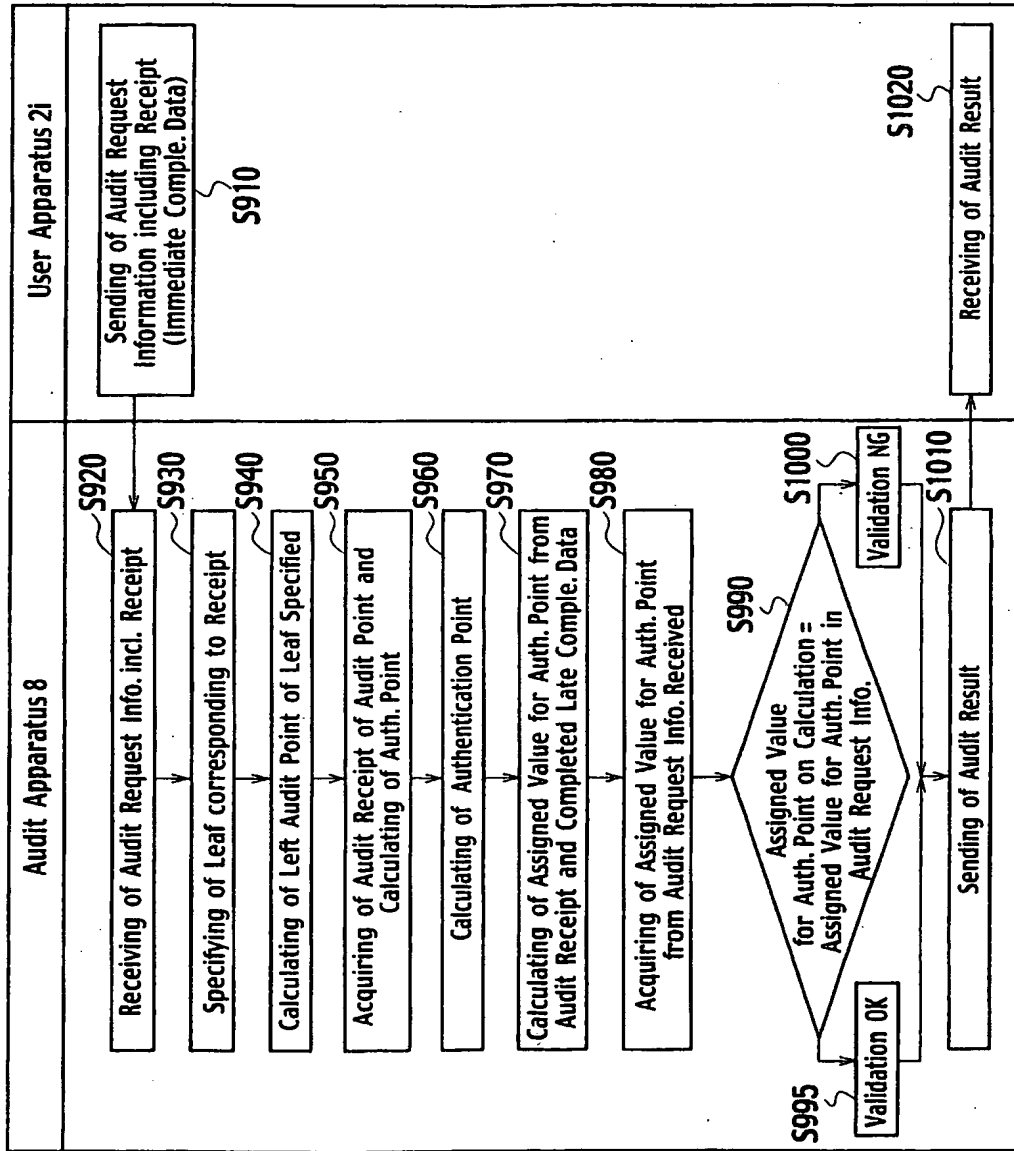


FIG. 17

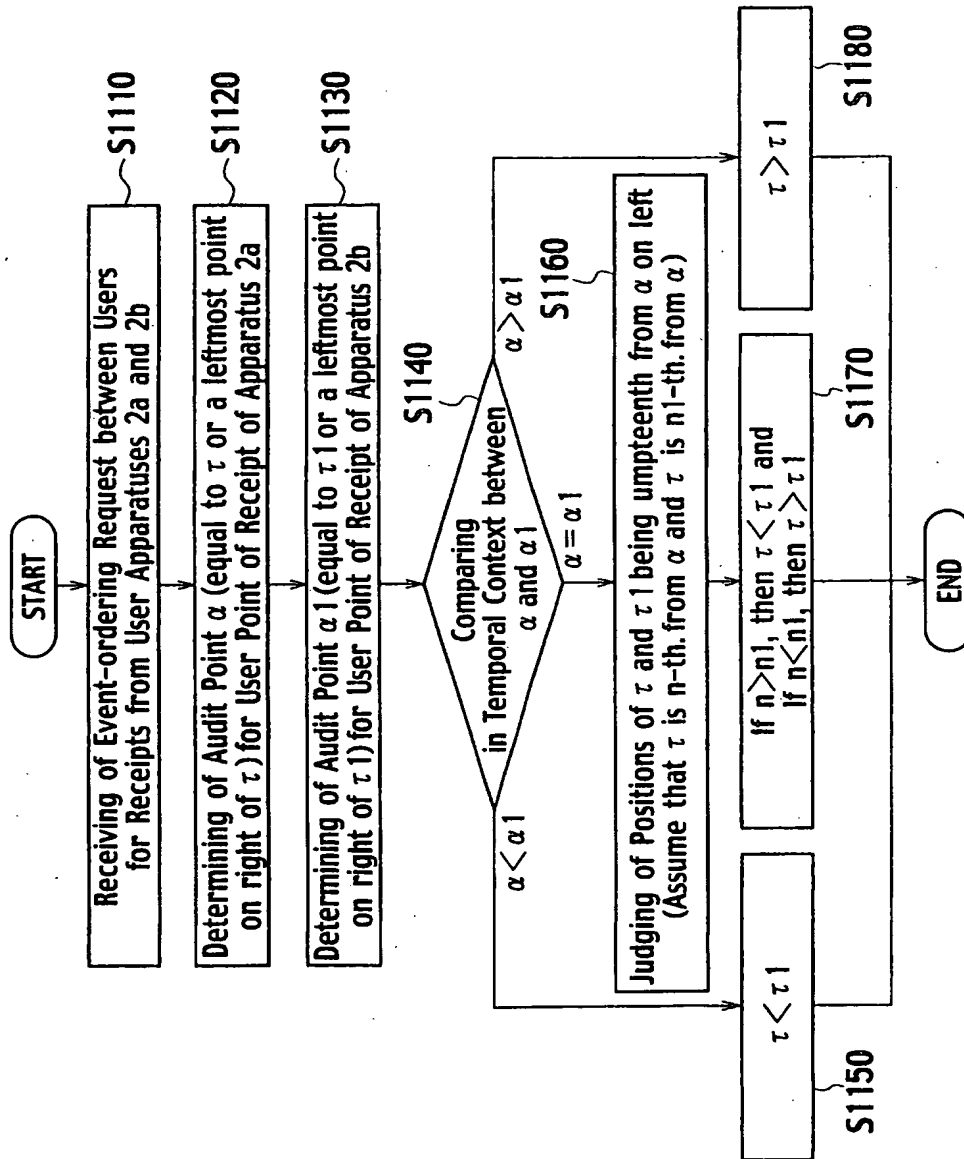


FIG. 18

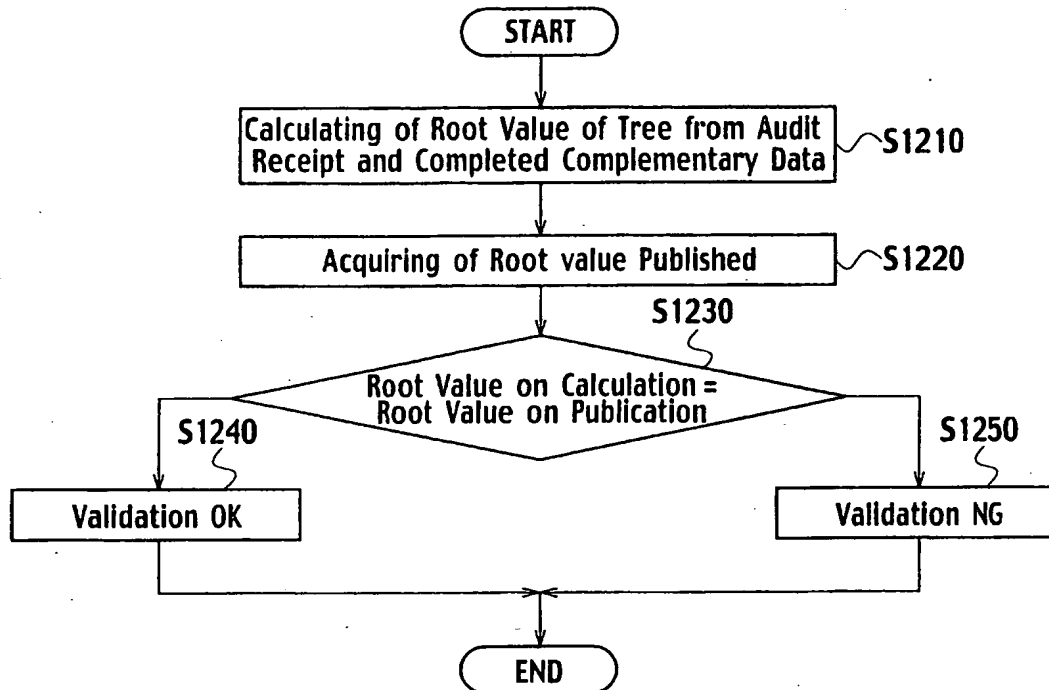


FIG. 19

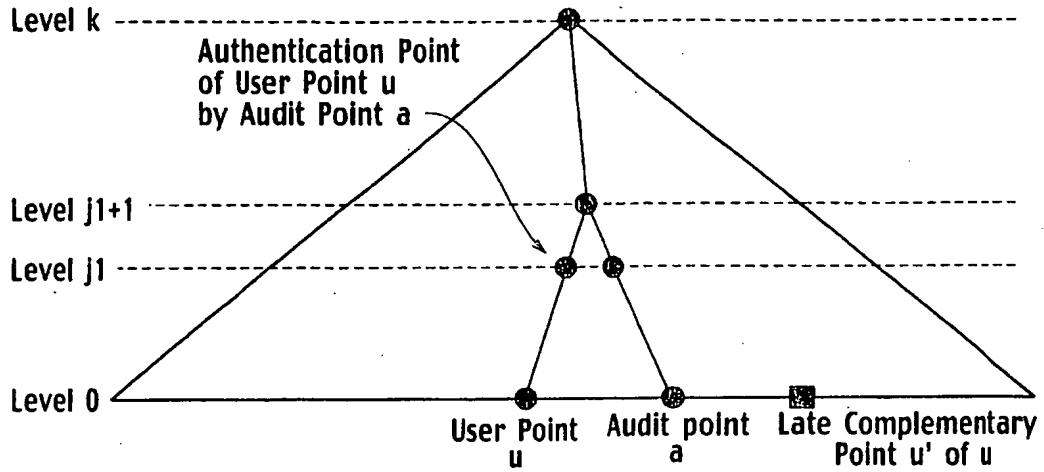


FIG. 20

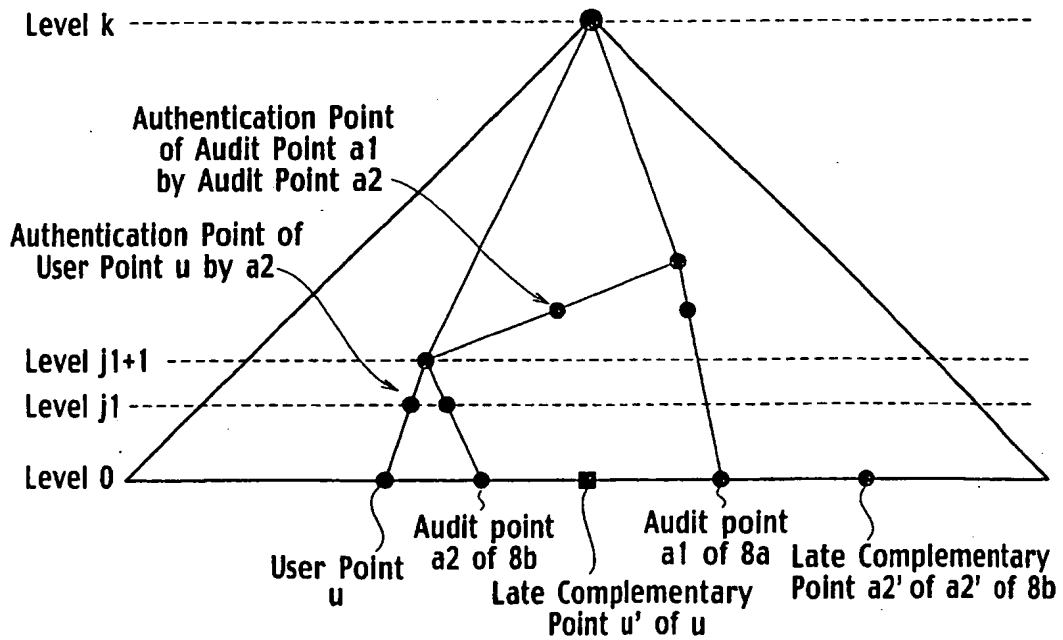
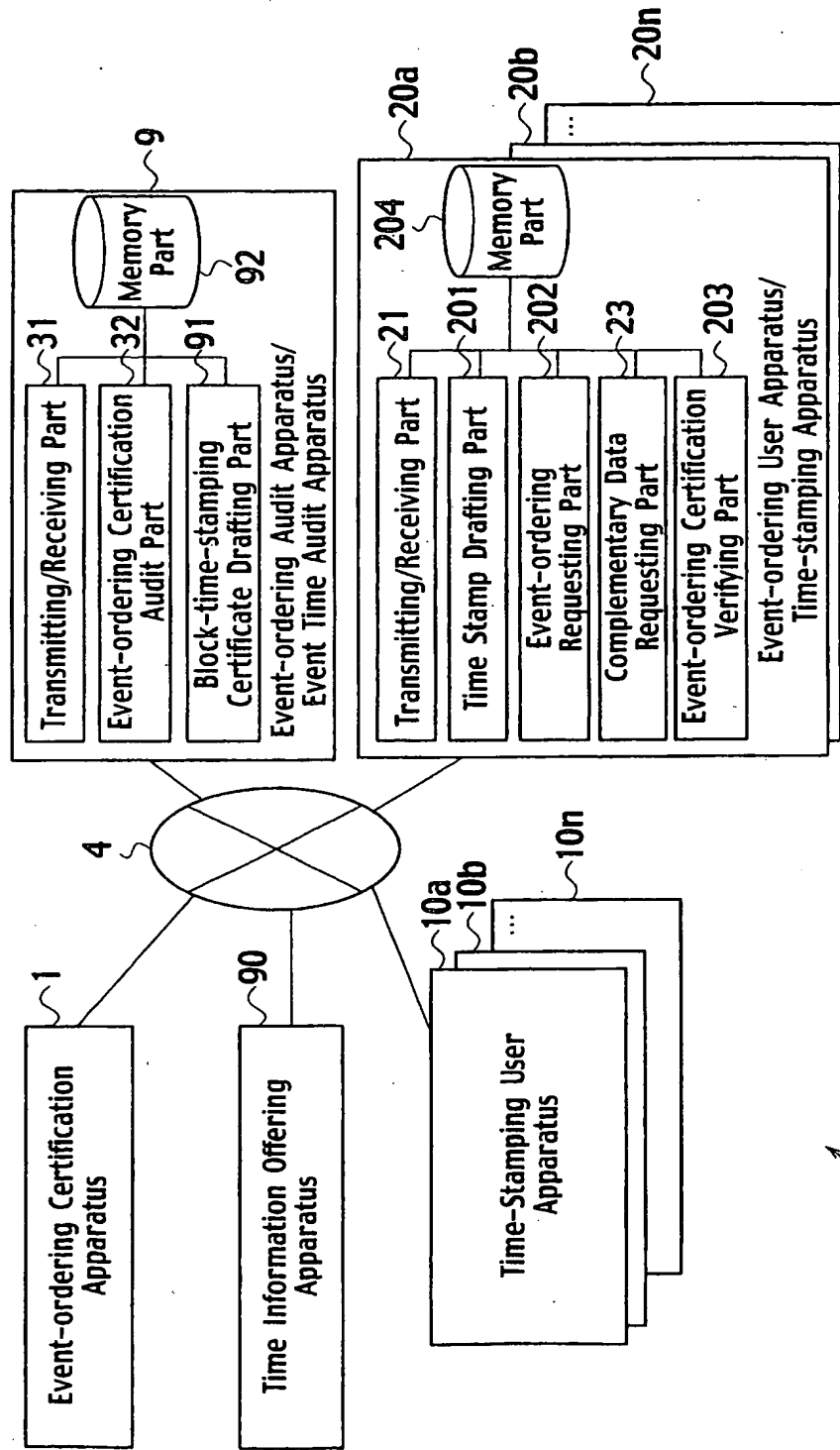


FIG. 21



300

FIG. 22

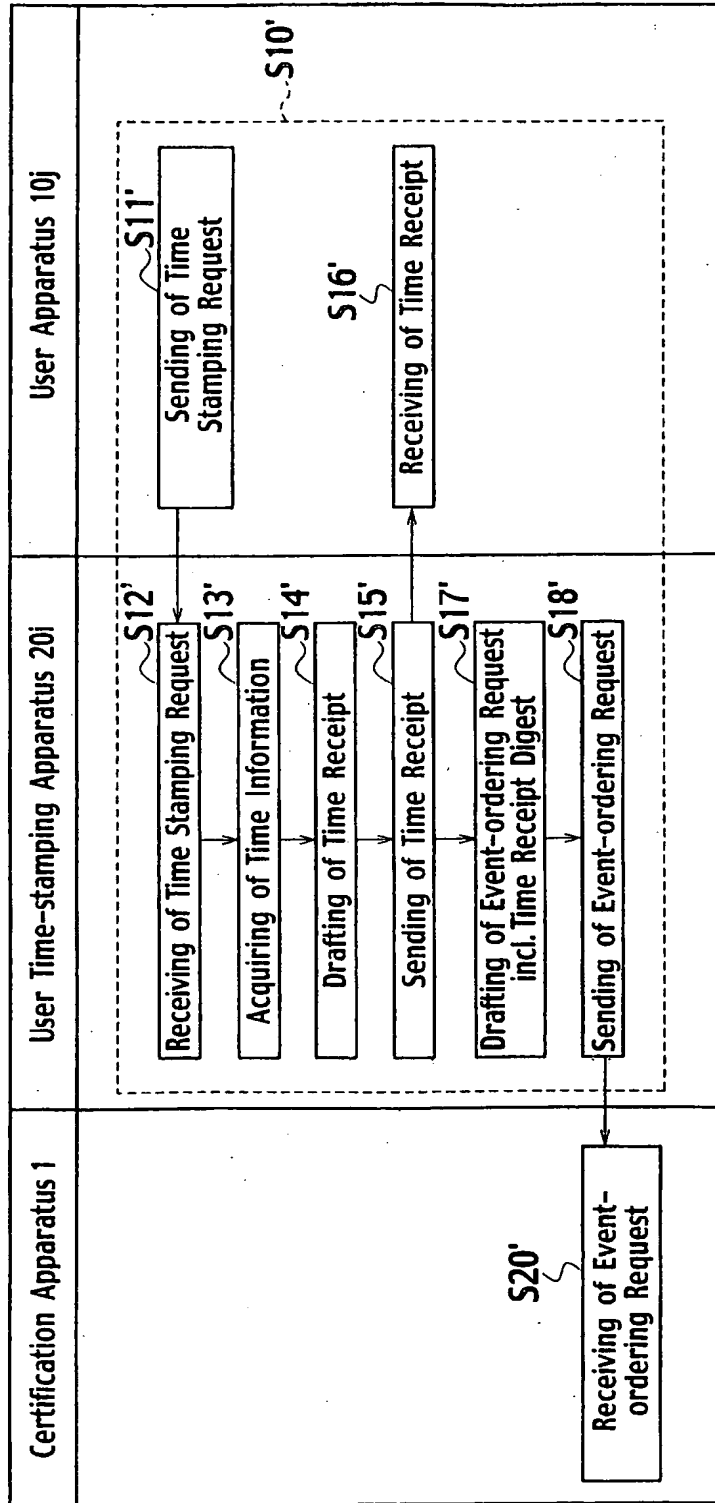


FIG. 23

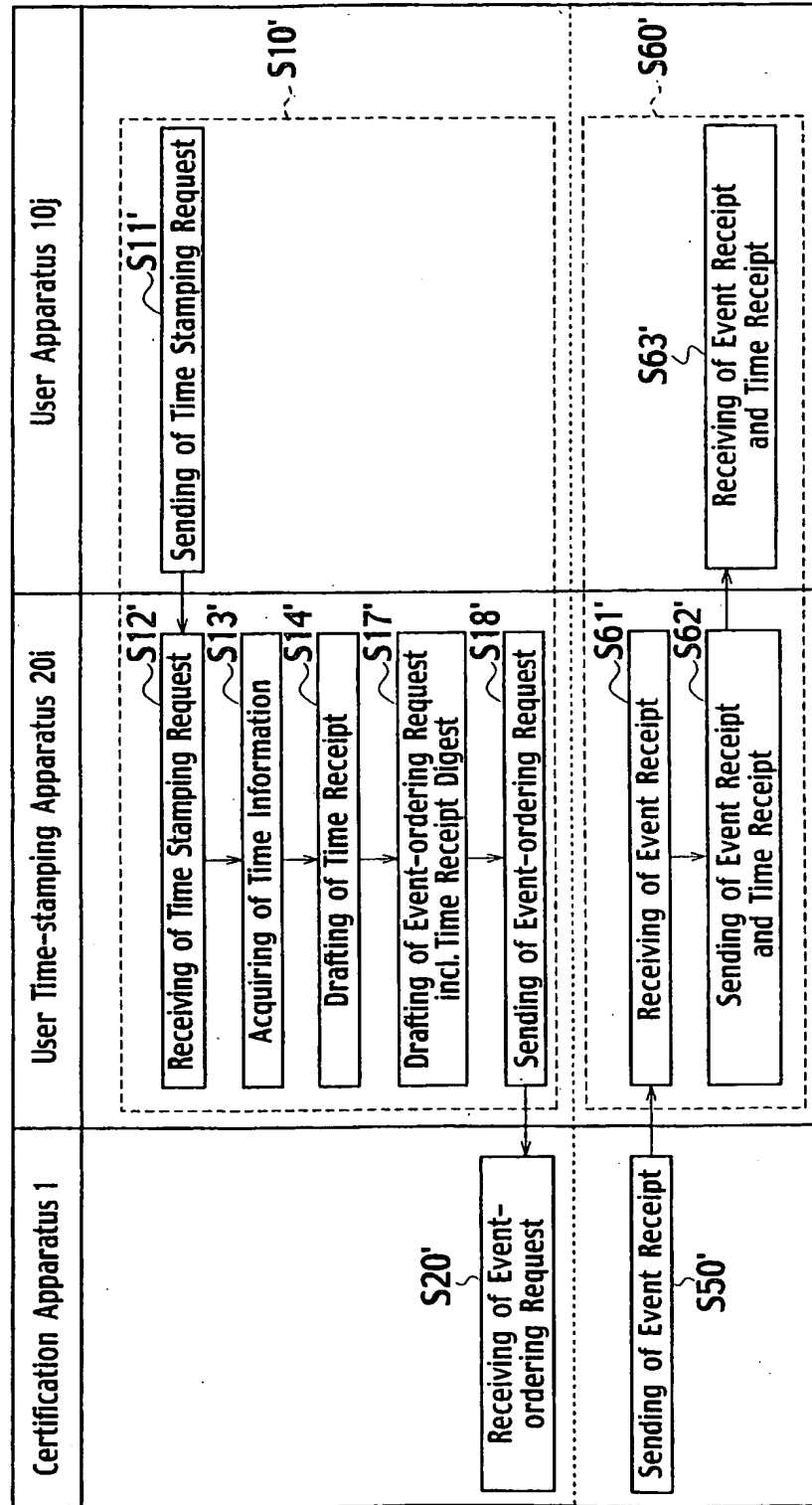


FIG. 24

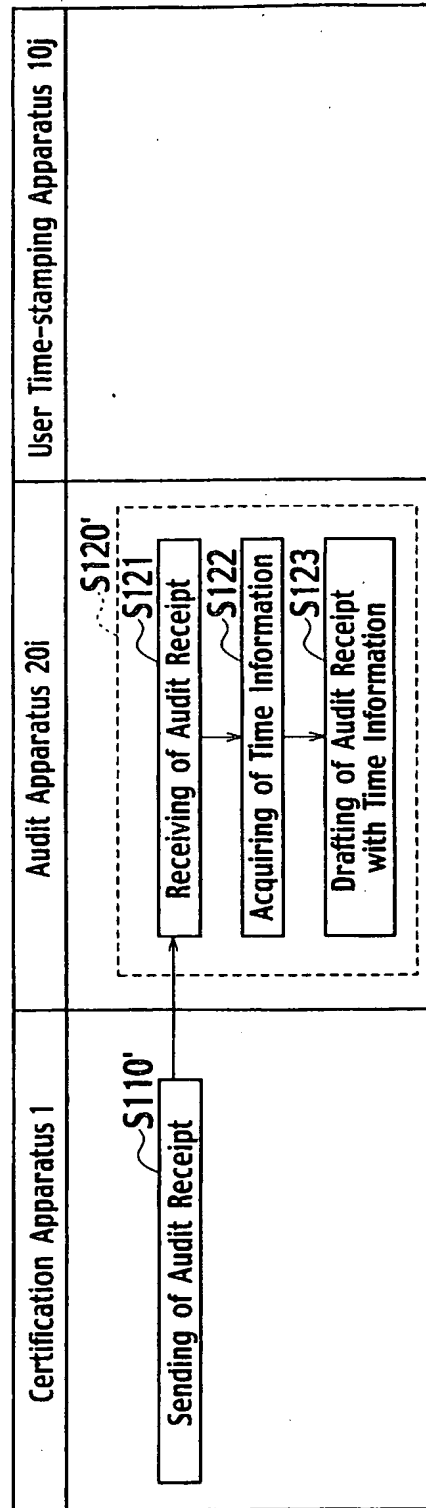




FIG. 25

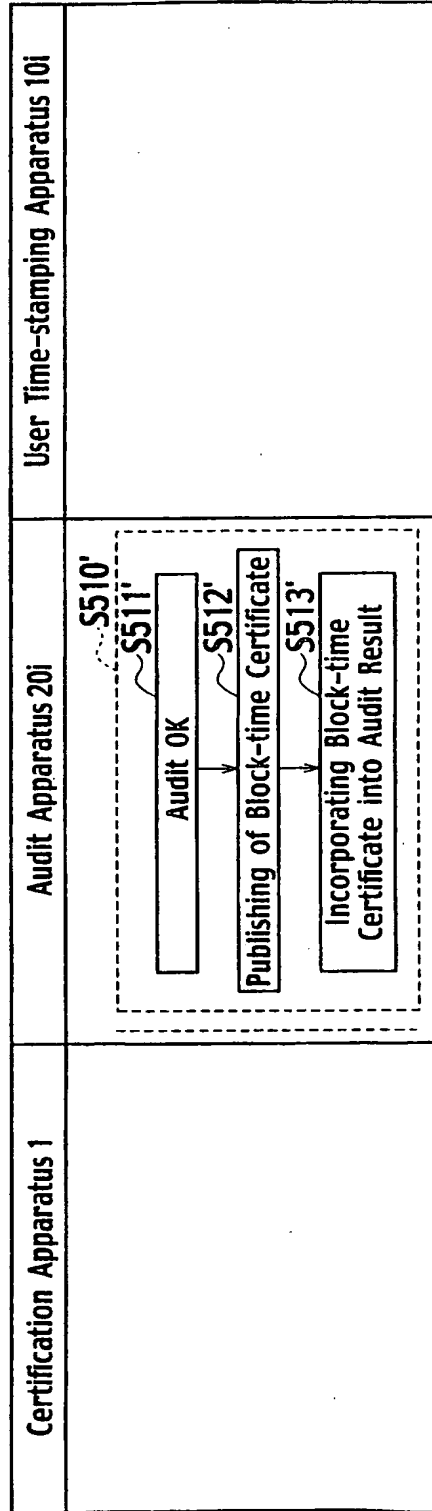


FIG. 26

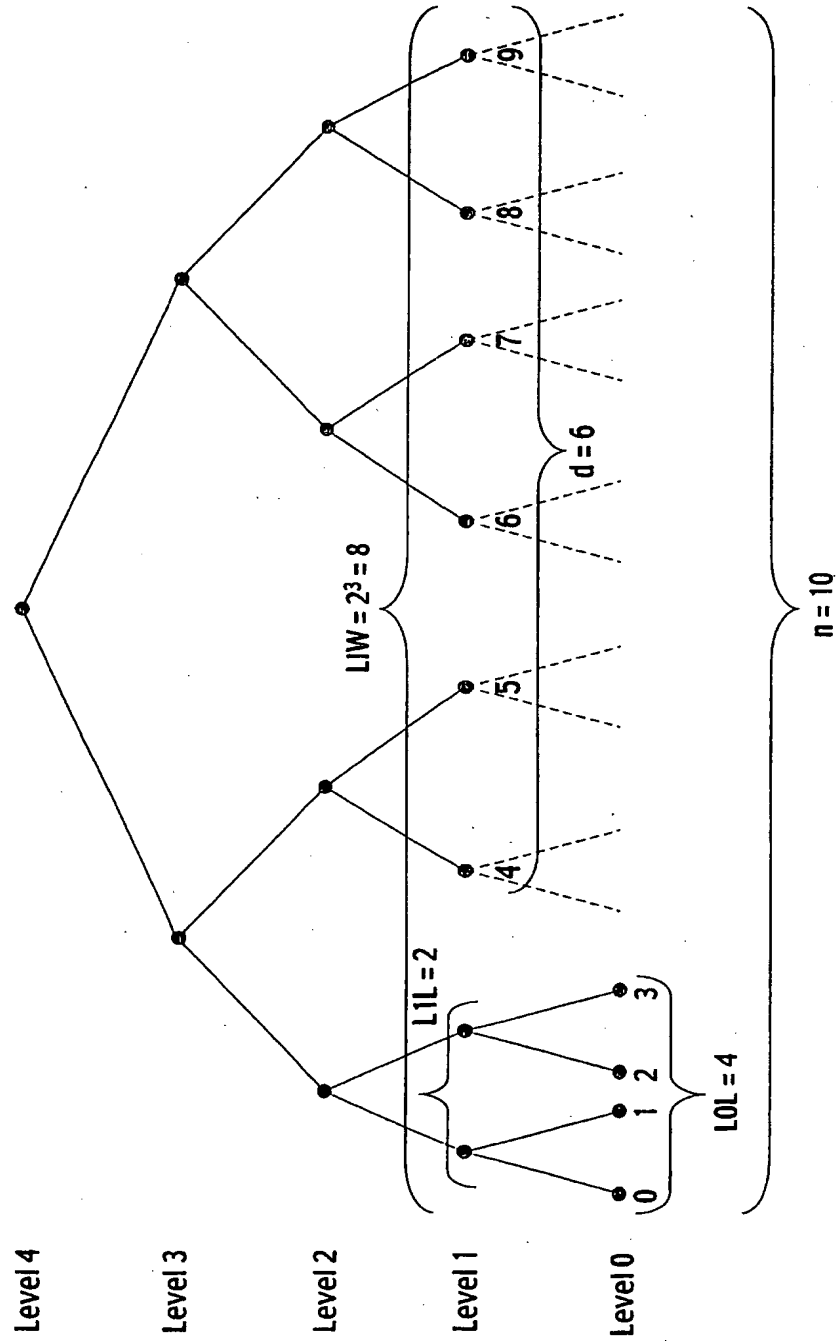


FIG. 27

(1) Loop 1: In a constructive method No. 3, the following processes are repeated until a regular time interval is completed.

- (1.1) Setting a request on acceptance to x
- (1.2) Increasing n by increment of 1
- (1.3) Loop 2: Performing of the follow processes for  $j=0, \dots, k$ 
  - (1.3.1)  $i \rightarrow i_j$
  - (1.3.2) When  $j = 0$ , set  $A_j[i] = x$ .  
(Set x to node(j,  $i_j$ .)
  - (1.3.3) When  $j > 0$ , perform as follows.
    - Set  $x_0 = A_{j-1}[\text{index}(\text{leftChild}(j, i))]$   
(Set  $x_0$  to an assigned value for left-child of node(j,  $i$ .)
    - Set  $x_1 = A_{j-1}[\text{index}(\text{rightChild}(j, i))]$   
(Set  $x_1$  to an assigned value for right-child of node(j,  $i$ .)
    - Calculate  $x_2 = h(x_0 \parallel x_1)$
    - Set  $A_j[i] = x_2$   
(Assign  $x_2$  to node(j,  $i$ .)
  - (1.3.4) Increasing  $i_j$  by increment of 1
  - (1.3.5) Withdraw from loop 2 if i is an even number.

Completion of loop 2  
Completion of loop 1

Processing Procedure 1

FIG. 28

(2) Performing of the following processes after withdrawing from loop 1 on reaching finish time.

- (2.1) Set  $k := \text{ceiling}(\log_2(n))$ .
- (2.2) Calculate  $\text{rtPath}(k, 0, n-1)$  and Set  $((0, r(0), \dots, k, r(k)))$  to the calculation result.
- (2.3) Loop 3: Performing of the follow processes for  $j=0, \dots, k$ 
  - (2.3.1)  $i \rightarrow i_j$
  - (2.3.2) Case of  $j = 0$ :
    - (2.3.2.1) When  $i$  is an odd number:
      - Produce a dummy  $r := R(0, i)$
      - Set  $A_j[i] := r$   
(Assign  $r$  to node(0,  $i$ ))
      - Set  $b_j := \text{true}$ .
      - Increase  $i_j$  by increment of 1.
  - (2.3.2) Case of  $0 < j \leq k$ :
    - (2.3.2.1) When  $i = r(j)$ :
      - (when node( $j, i$ ) is on  $\text{rtPath}(k, 0, n-1)$ ):
      - (2.3.2.1.1)  $x_0 := A_{j-1}[\text{Index}(\text{leftChild}(j, i))]$   
(Set  $x_0$  to an assigned value for left-child of node( $j, i$ ))
      - (2.3.2.1.2)  $x_1 := A_{j-1}[\text{Index}(\text{rightChild}(j, i))]$   
(Set  $x_1$  to an assigned value for right-child of node( $j, i$ ))
      - (2.3.2.1.3) Calculate  $x_2 := h(x_0 \parallel x_1)$
      - (2.3.2.1.4) Set  $A_j[i] := x_2$   
(Assign  $x_2$  to node( $j, i$ ))
    - (2.3.2.1.5) When  $i$  is an even number and  $j < k$ :
      - Increase  $i$  by increment of 1.
      - Calculate  $r := R(j, i)$  and Set  $A_j[i] := r$   
(Assign  $r$  to node( $j, i$ ))
      - Set  $b_j := \text{true}$ .
      - Set  $i_j := i + 1$
    - (2.3.2.2) When  $i = r(j) + 1$ , an odd number and  $j < k$ :
      - Calculate  $r := R(j, i)$  and Set  $A_j[i] := r$   
(Assign  $r$  to node( $j, i$ ))
      - Set  $b_j := \text{true}$ .
      - Increase  $i_j$  by increment of 1.

Completion of loop 3

FIG. 29

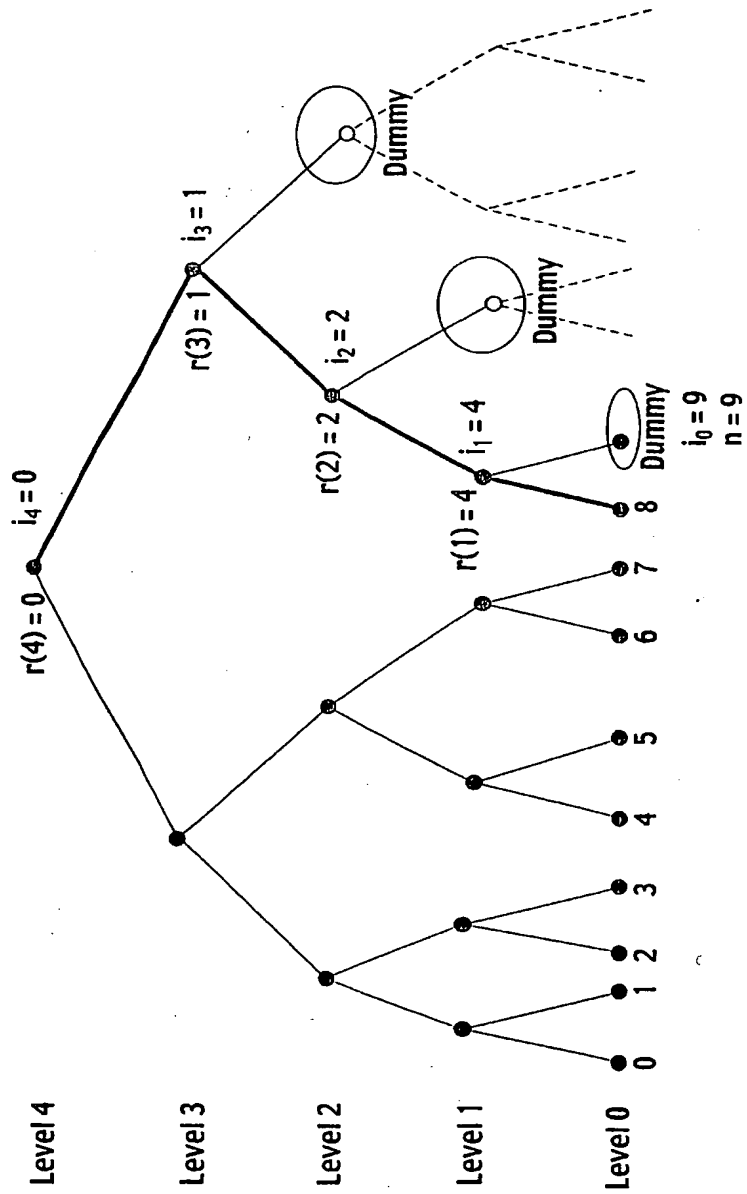




FIG. 31

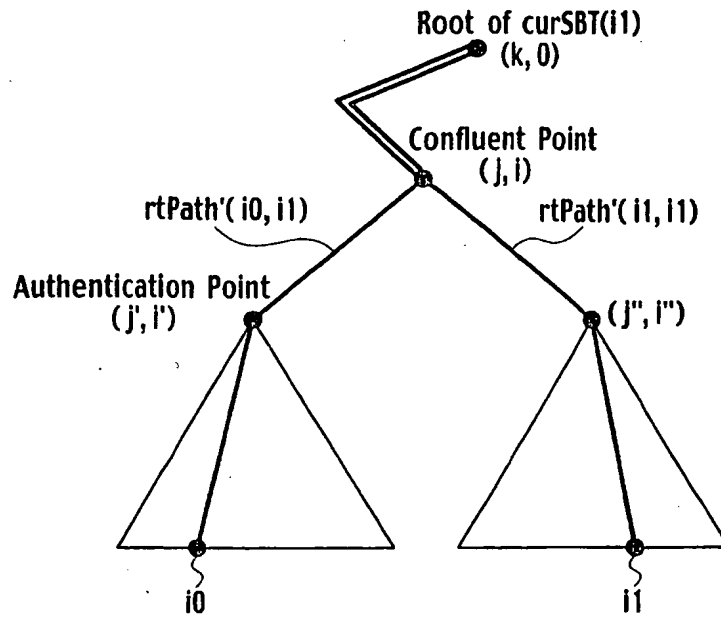


FIG. 32

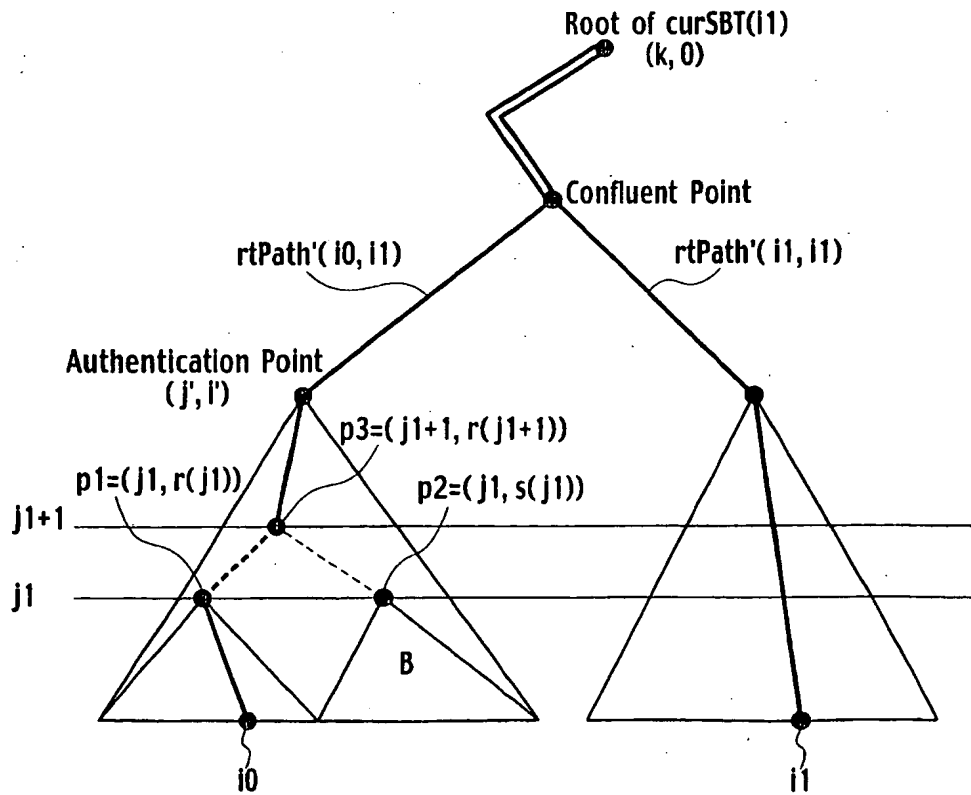


FIG. 33

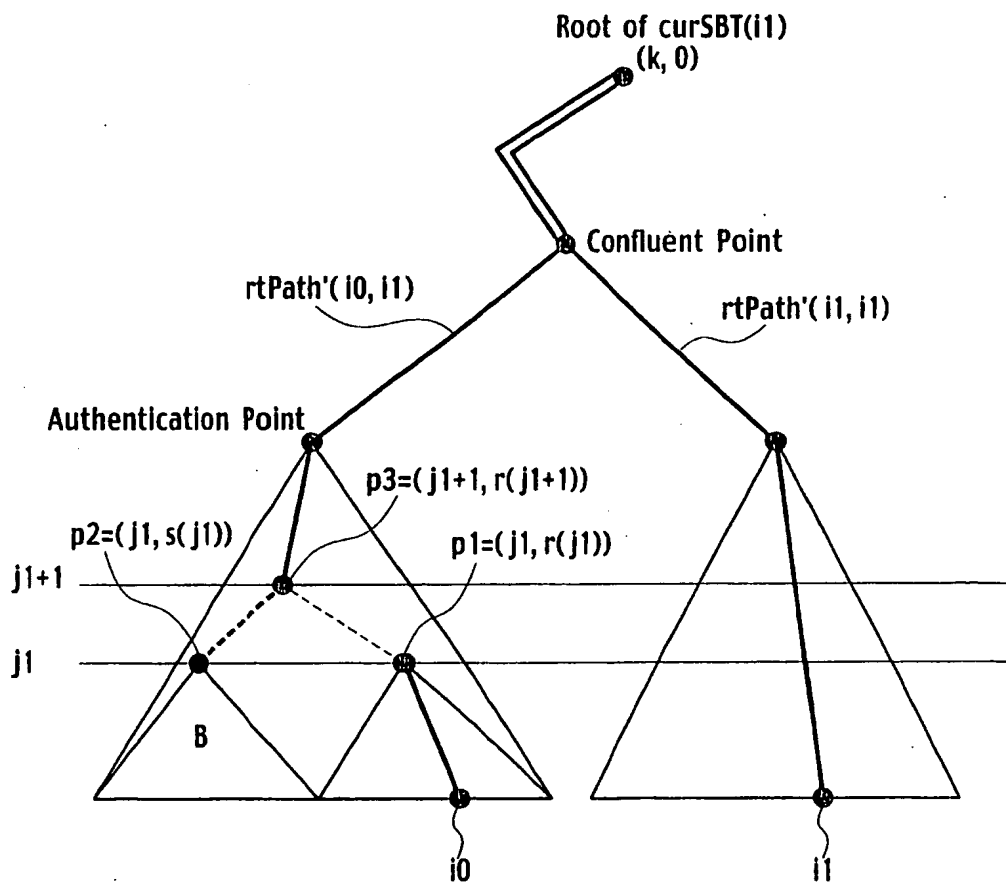




FIG. 34

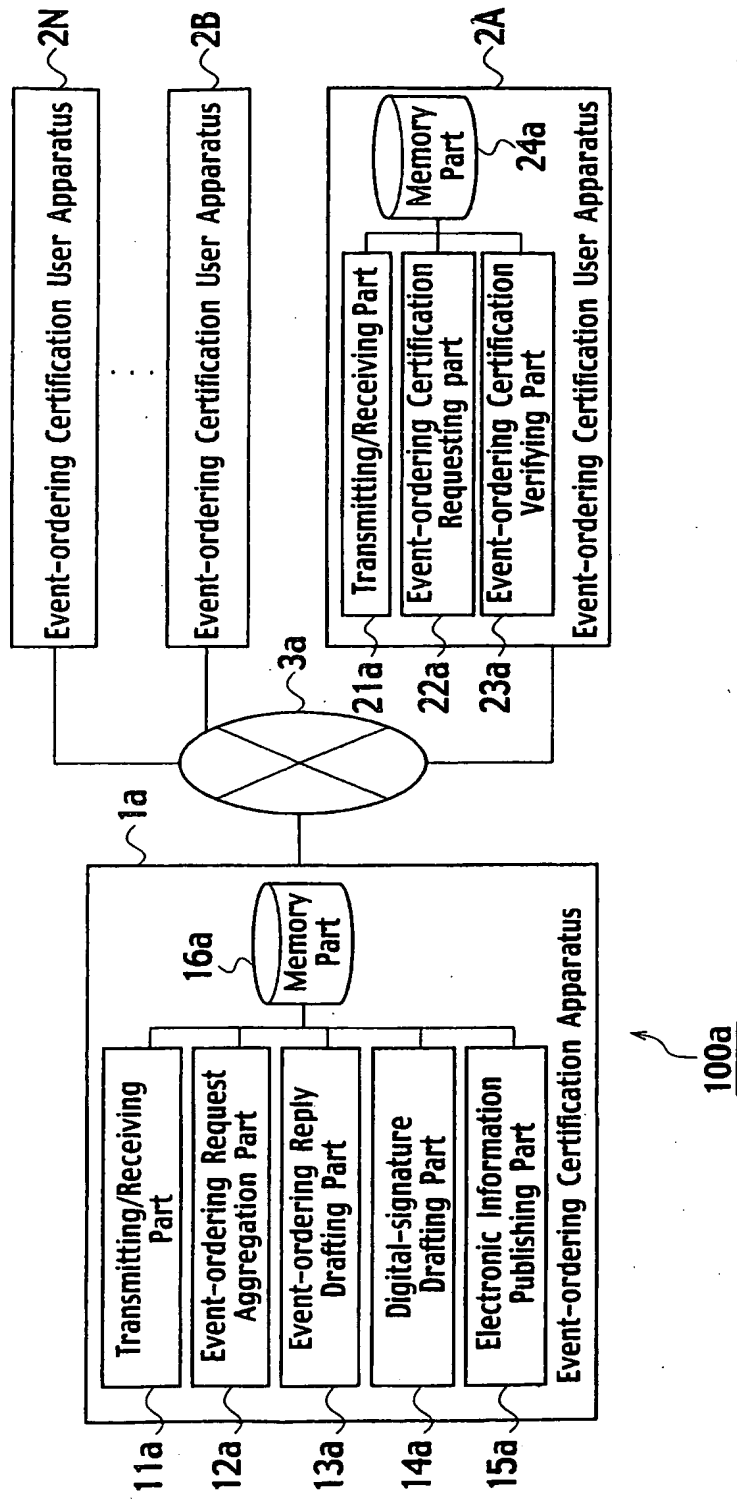


FIG. 35

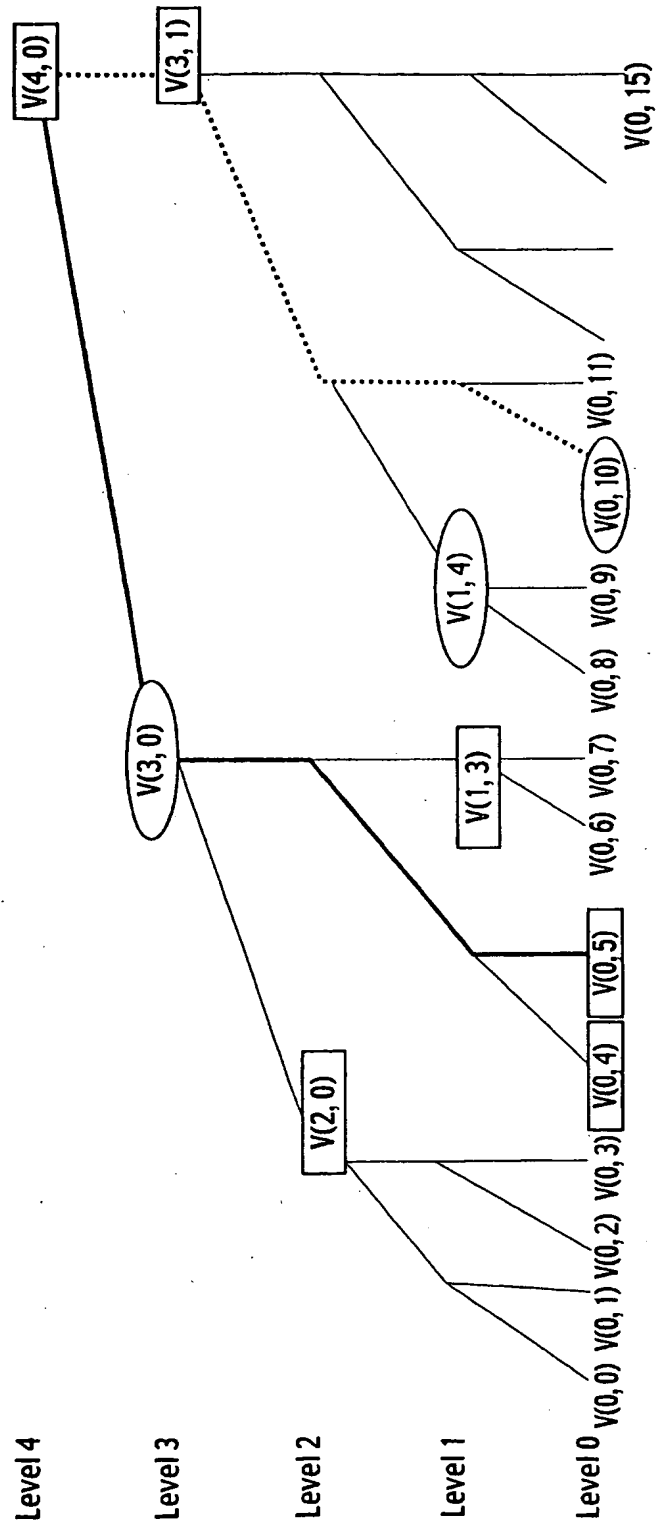


FIG. 36

ITEM	SIGN	REQUIRED
Original Data	Y	<input type="radio"/>
Sequentially Assigned Data-item	Z	<input type="radio"/>
Sequential Aggregation Tree No.	n	<input type="radio"/>
Sequential Aggregation Tree Leaf No.	i	<input type="radio"/>
Immediate Complementary Data of Registration Point (Positional Information Assigned Value)	SK	<input type="radio"/>
Late Complementary Data of Each Past Registration Point (Positional Information Assigned Value)	TK	<input type="radio"/>

Event-ordering Receipt  
EOC(y)

FIG. 37

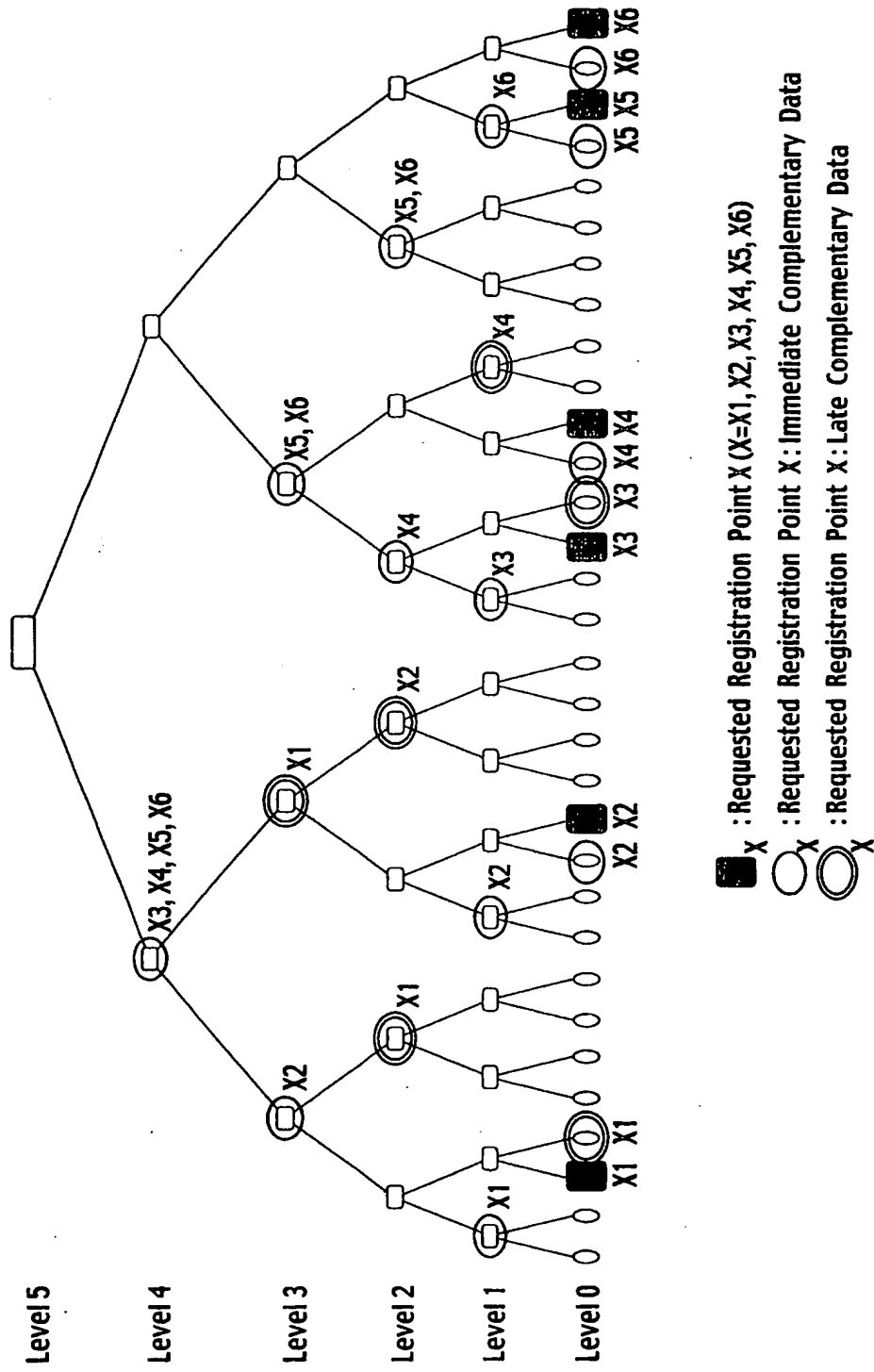


FIG. 38

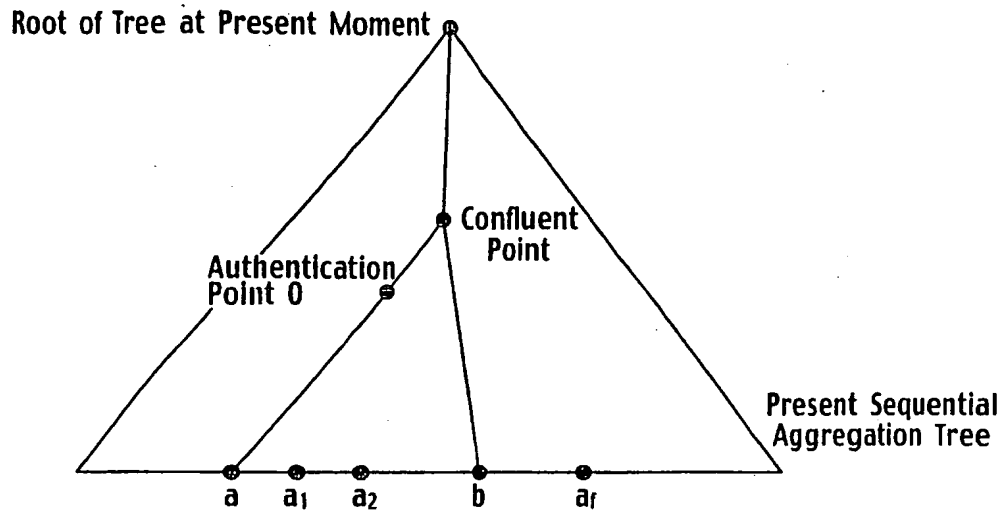


FIG. 39

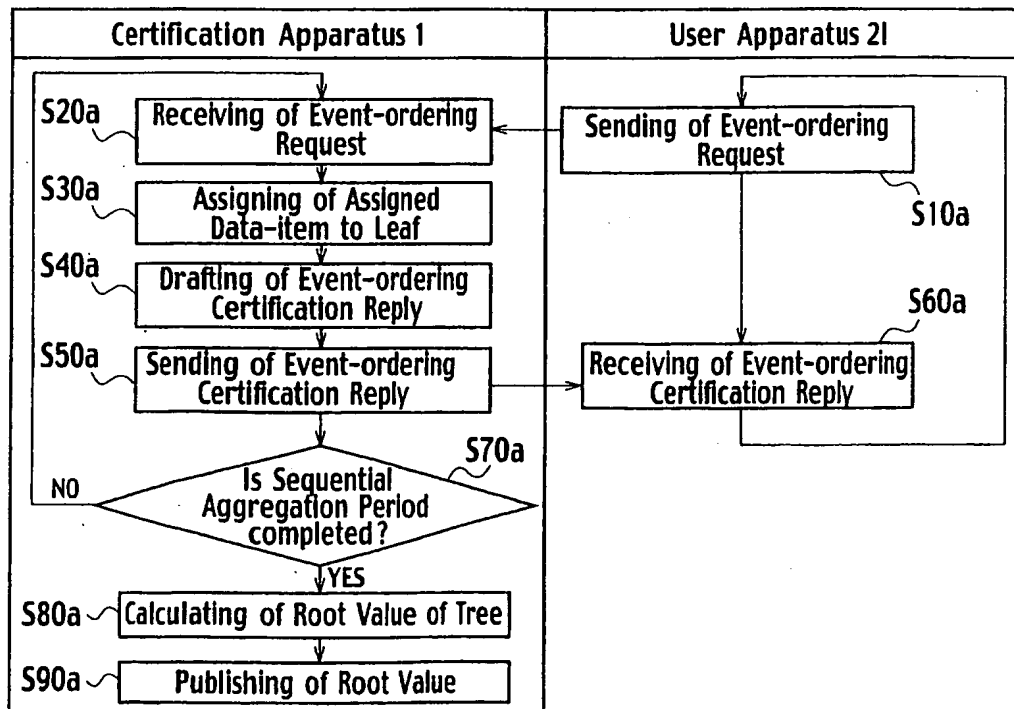


FIG. 40

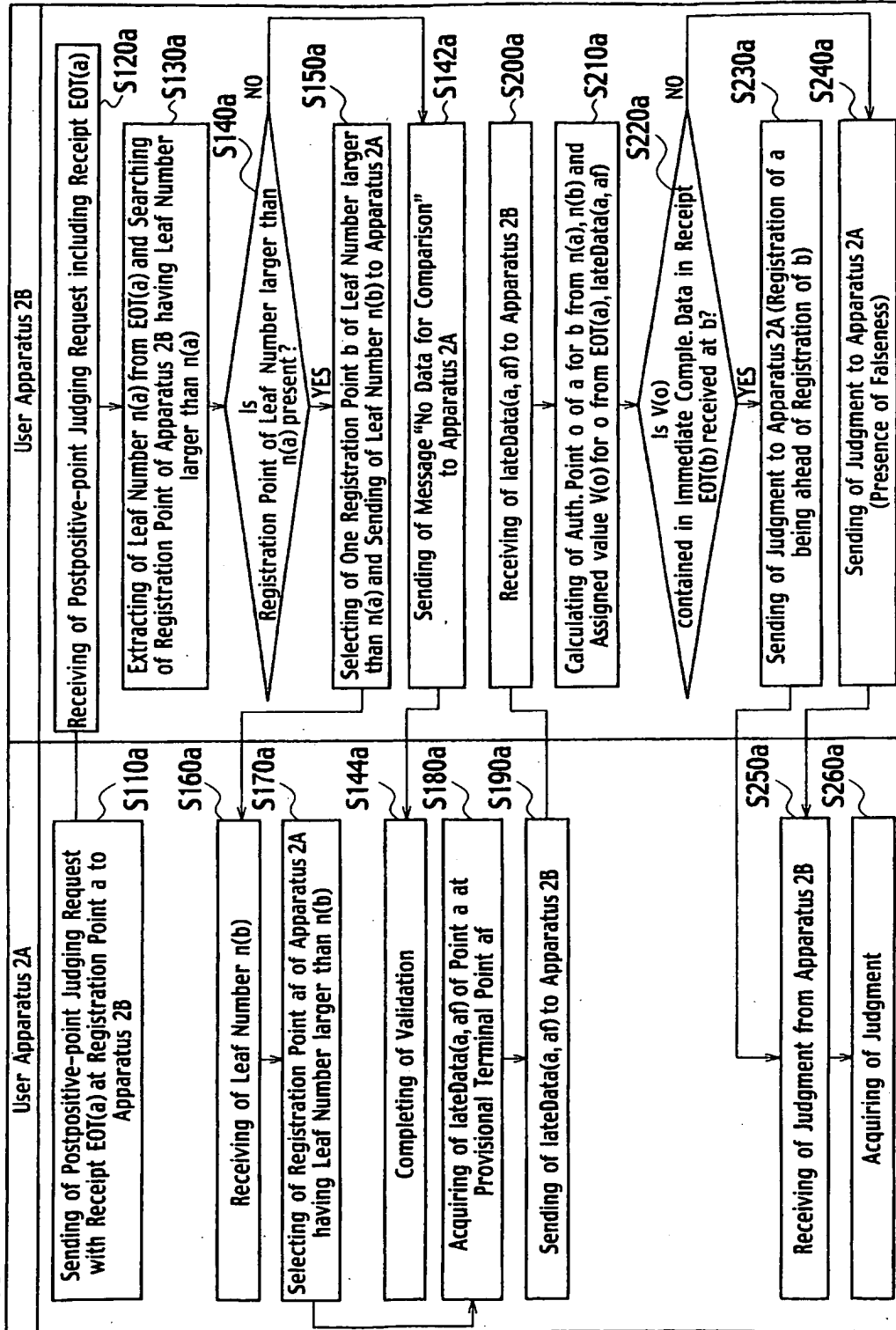


FIG. 41

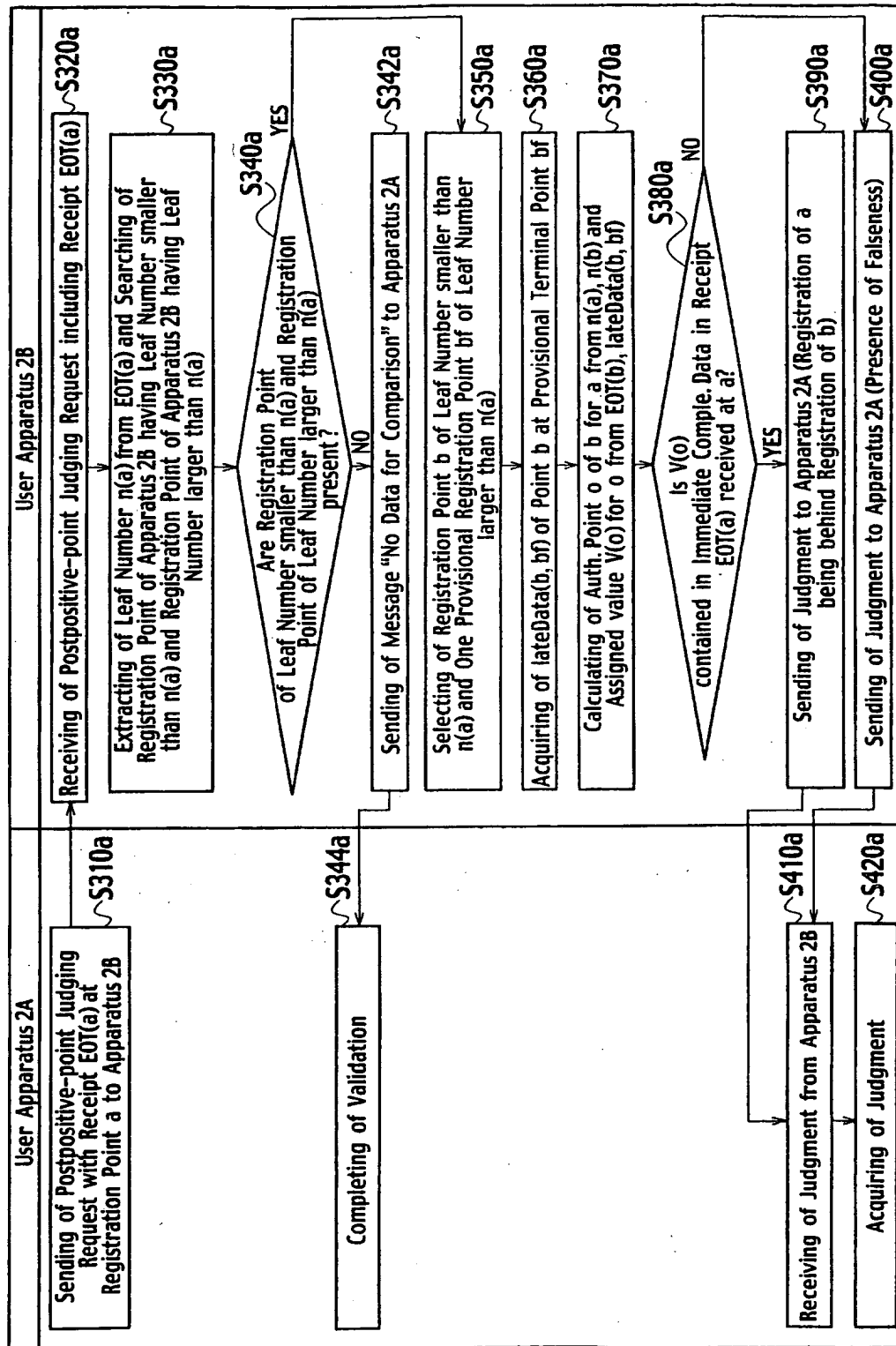
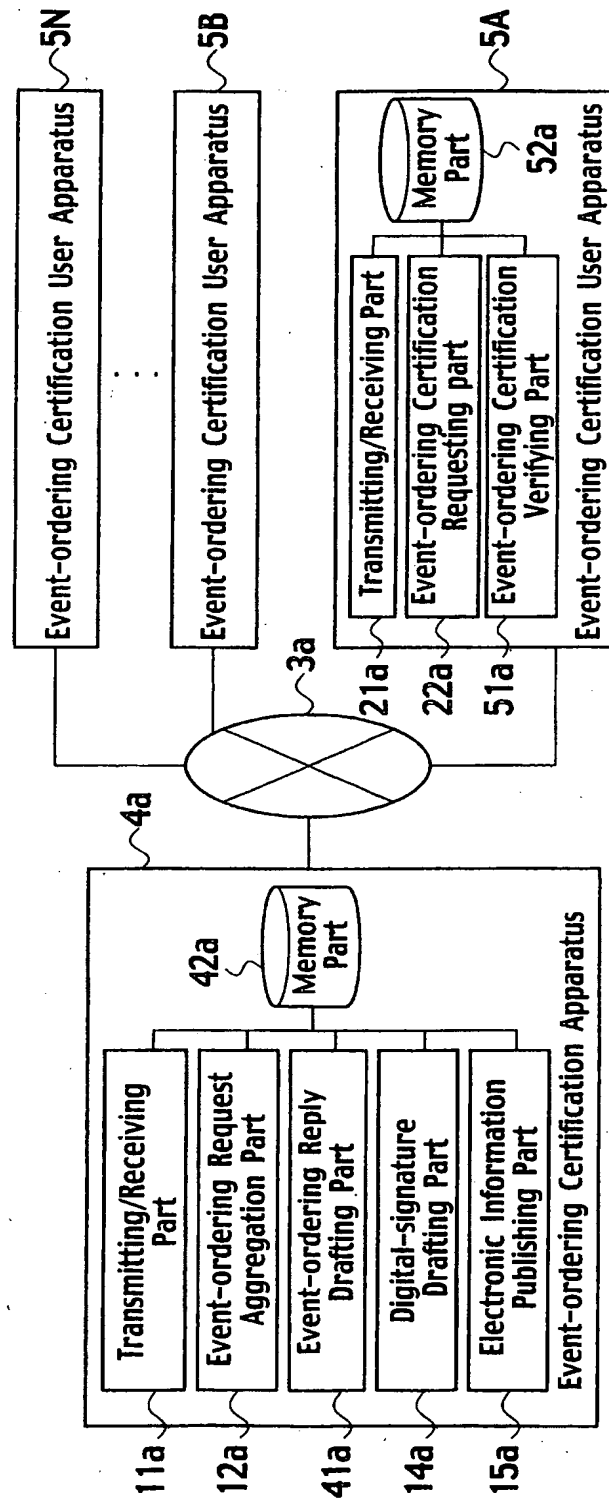


FIG. 42



200a



FIG. 43

ITEM	SIGN	REQUIRED
Original Data	y	<input type="radio"/>
Sequentially Assigned Data-Item	z	<input type="radio"/>
Sequential Aggregation Tree No.	n	<input type="radio"/>
Sequential Aggregation Tree Leaf No.	i	<input type="radio"/>
Immediate Complementary Data of Registration Point (Positional Information Assigned Value)	SK	<input type="radio"/>
Late Complementary Data of Immediately-preceding Registration Point (Positional Information Assigned Value)	TK2	<input type="radio"/>

} Event-ordering Receipt EOC(y)

FIG. 44

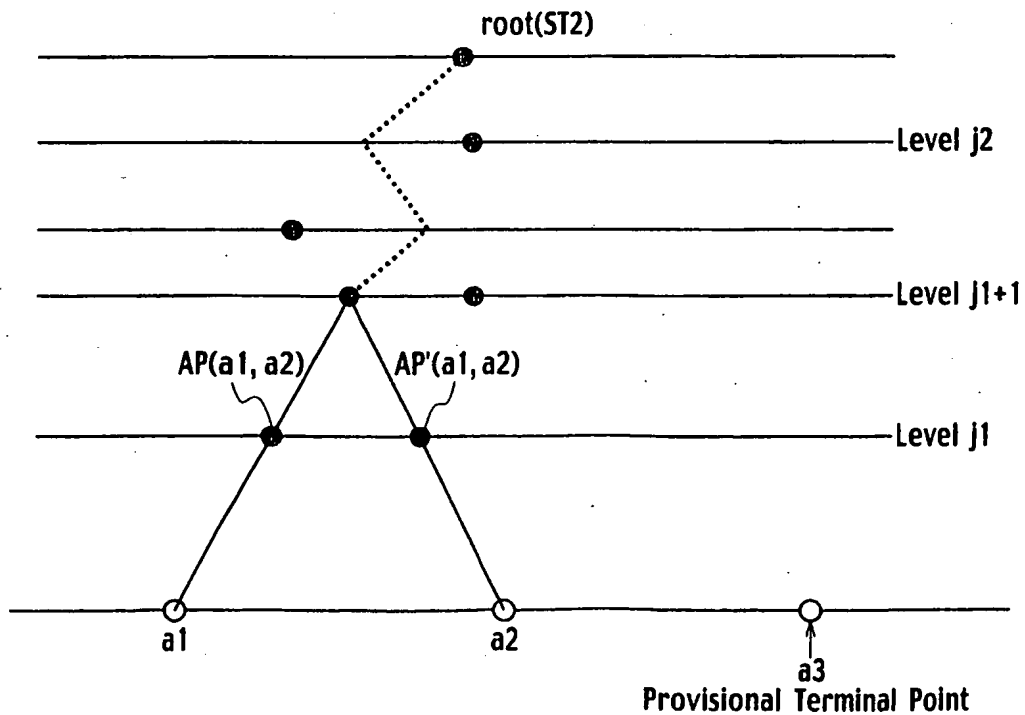


FIG. 45

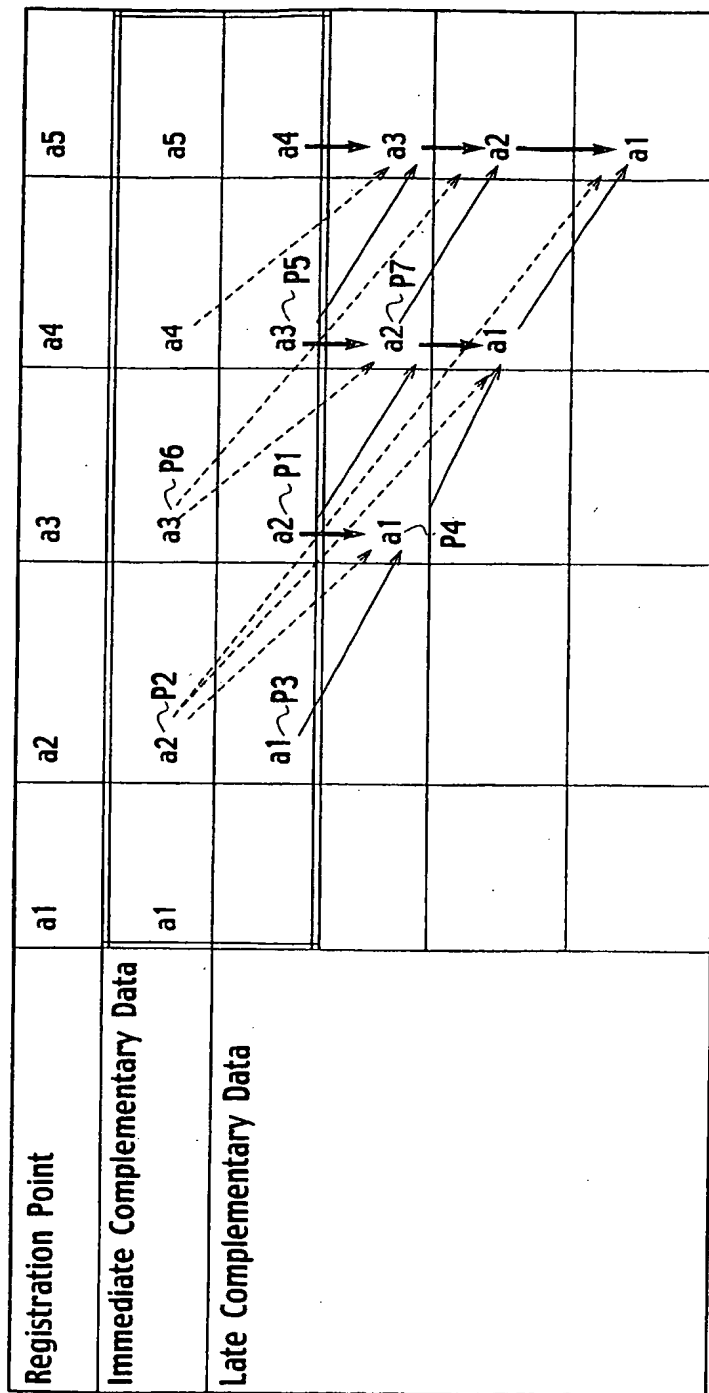


FIG. 46

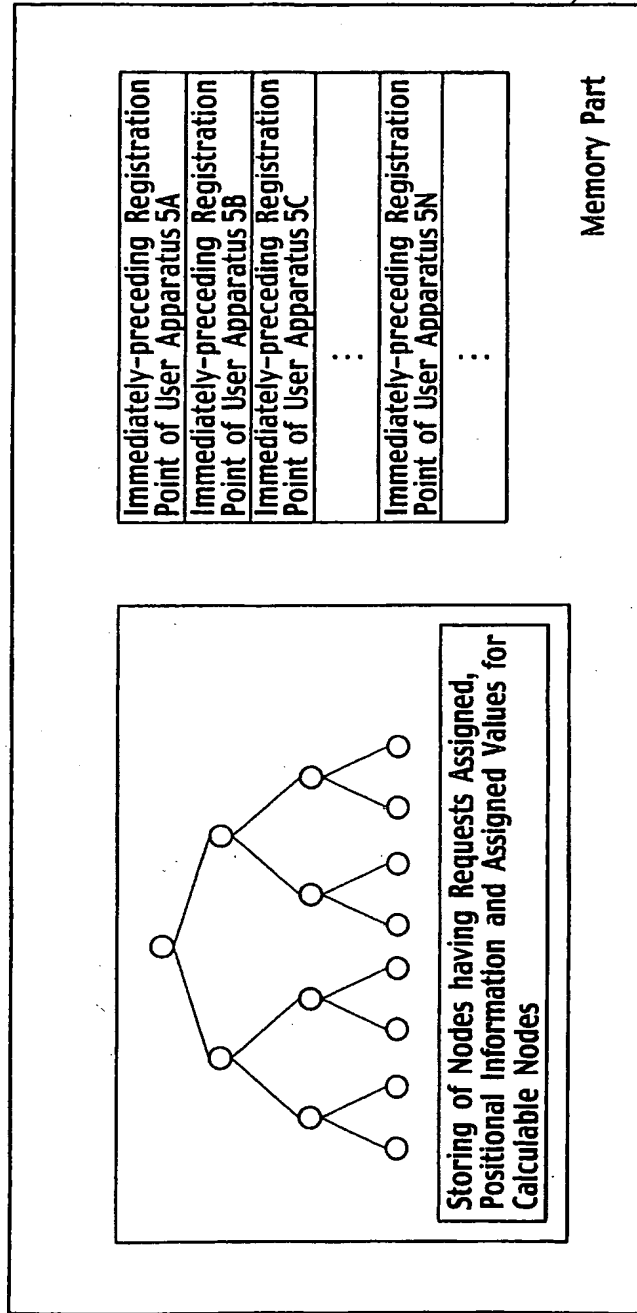


FIG. 47

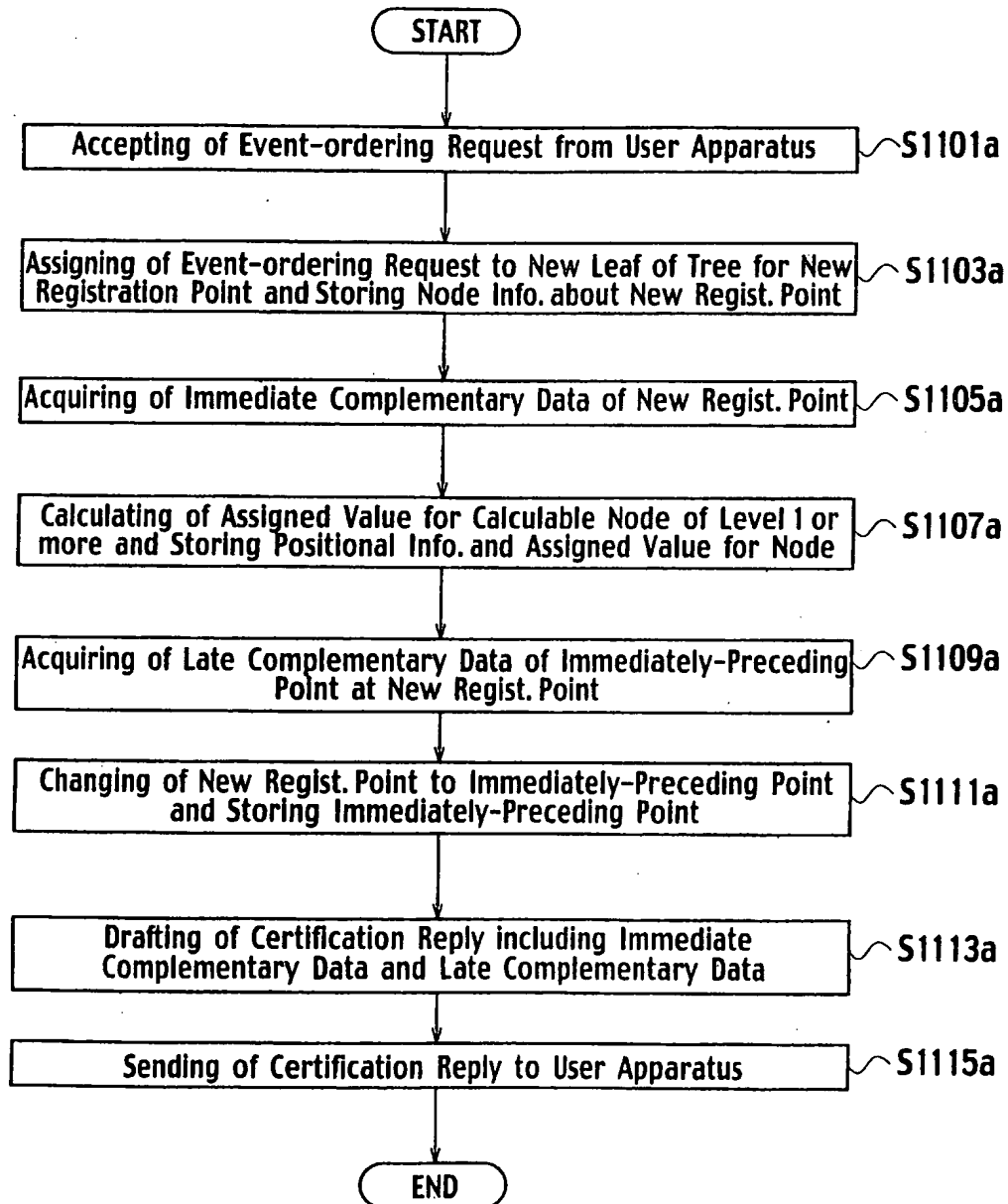
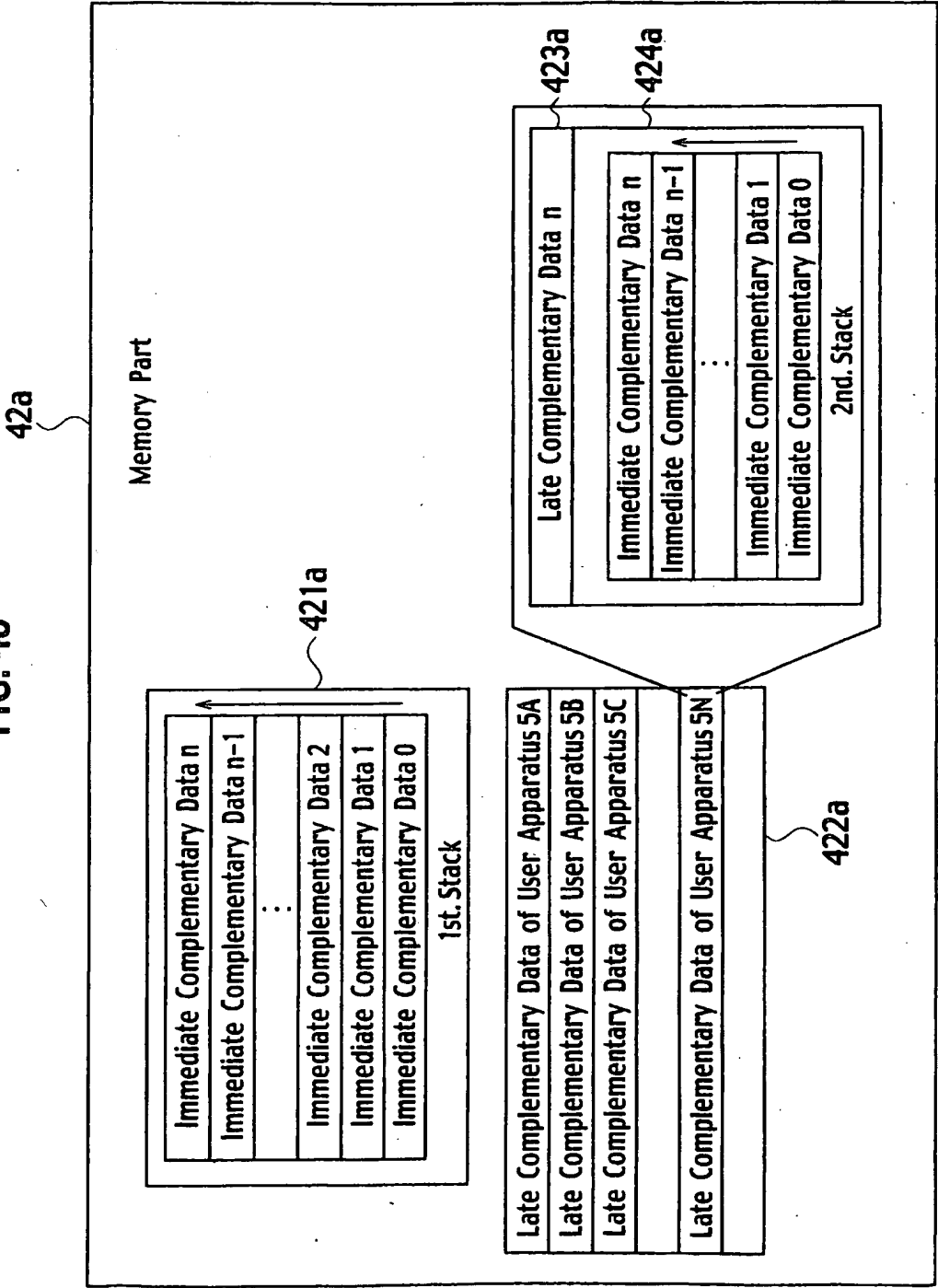


FIG. 48



44/77  
FIG. 49

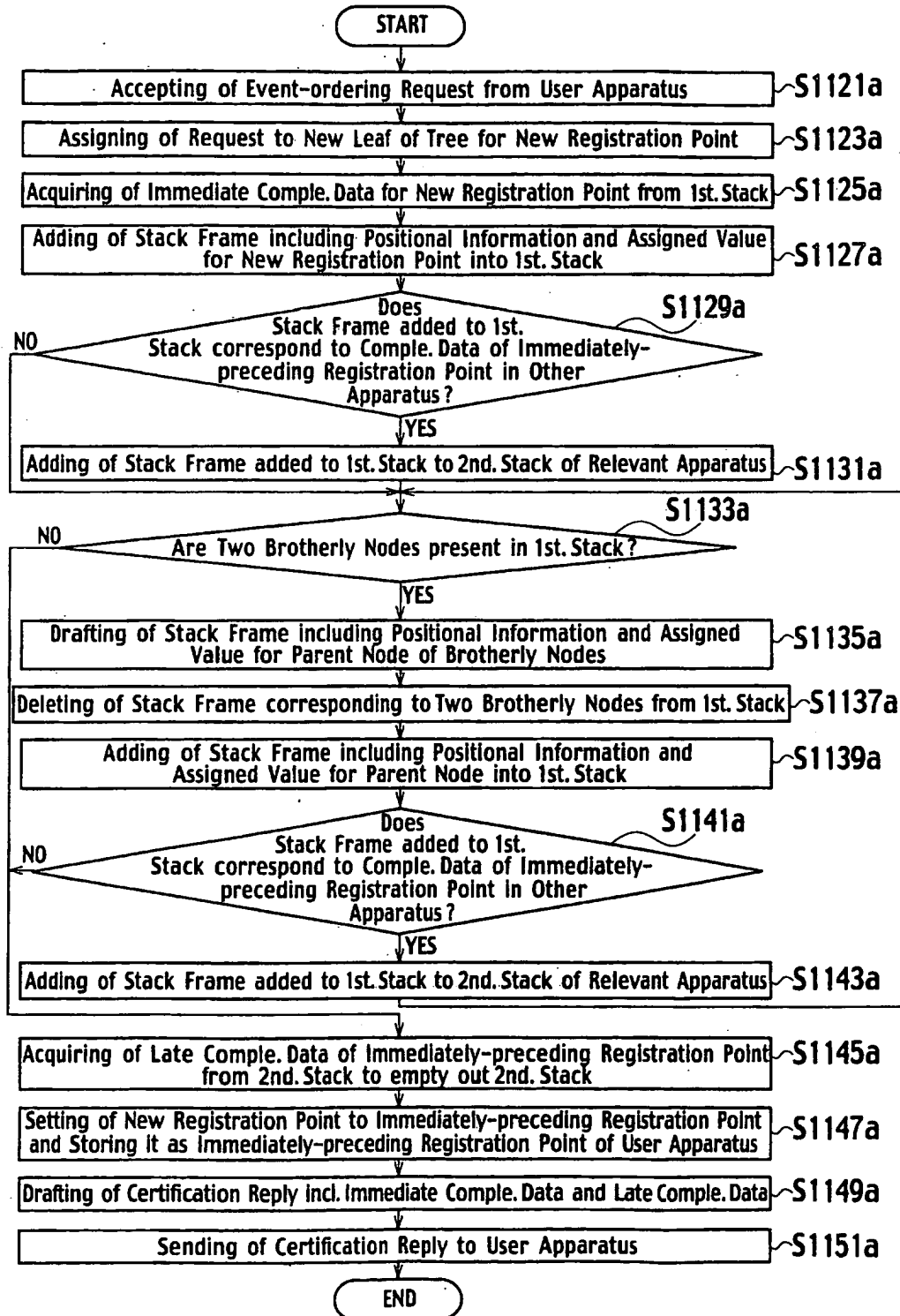


FIG. 50

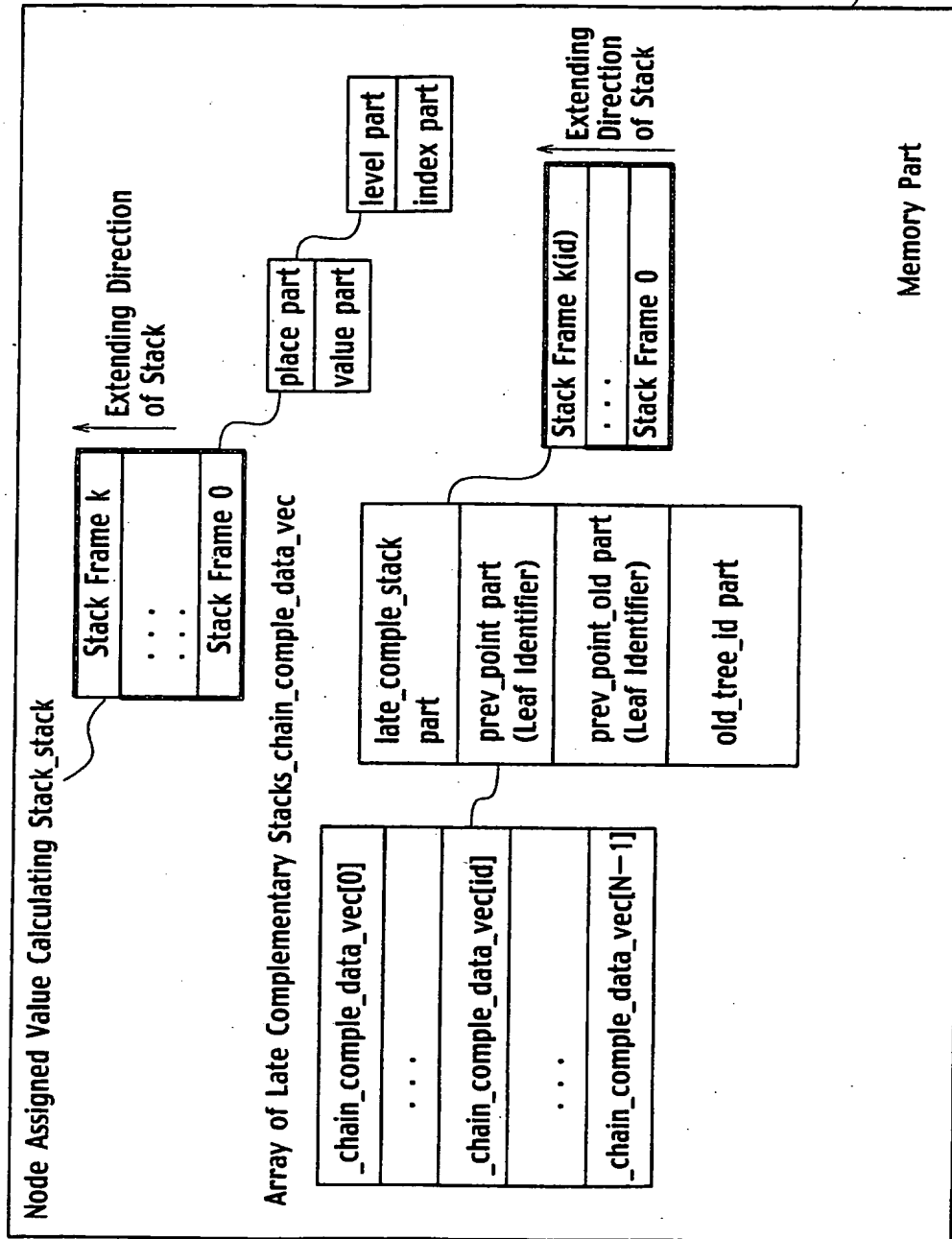
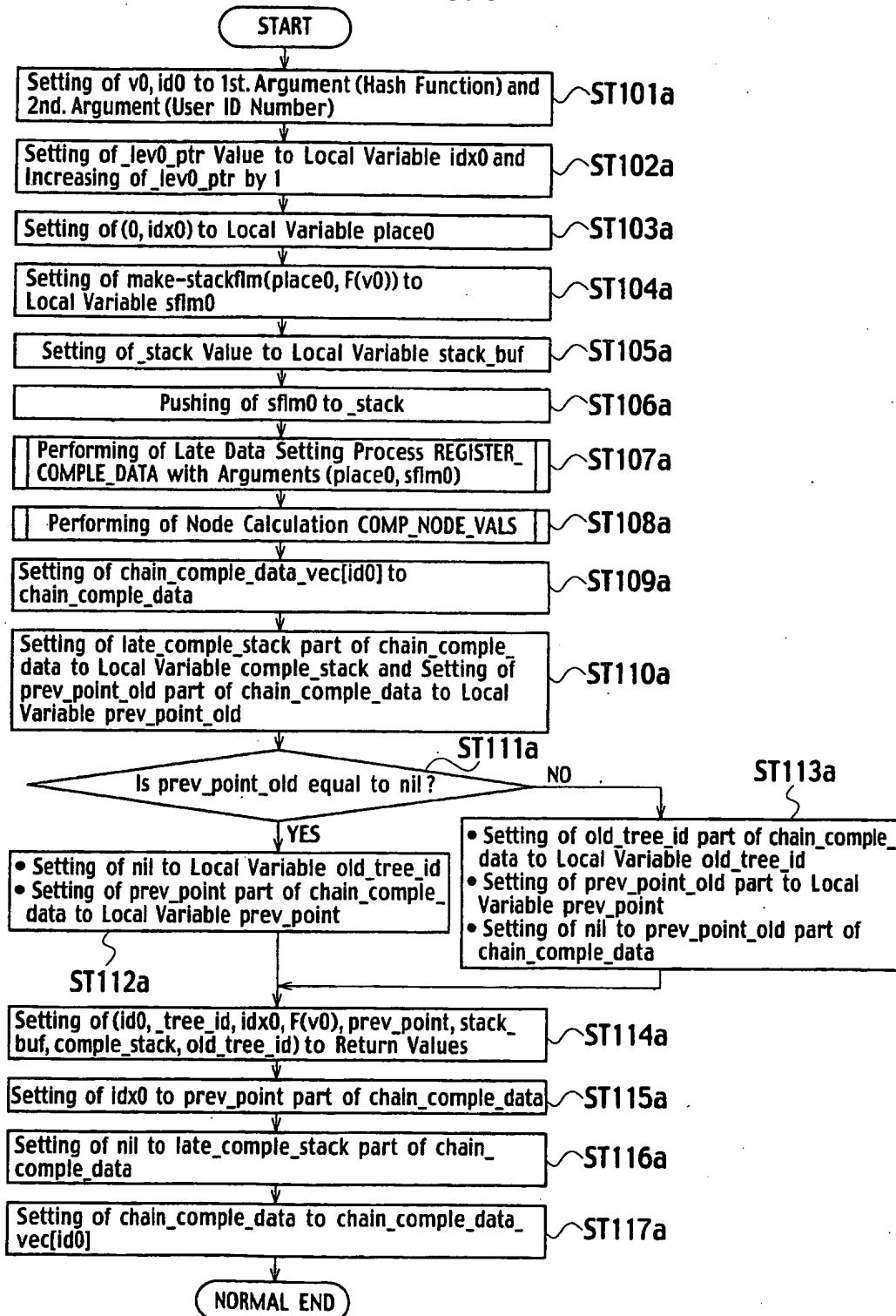


FIG. 51





47 / 77  
FIG. 52

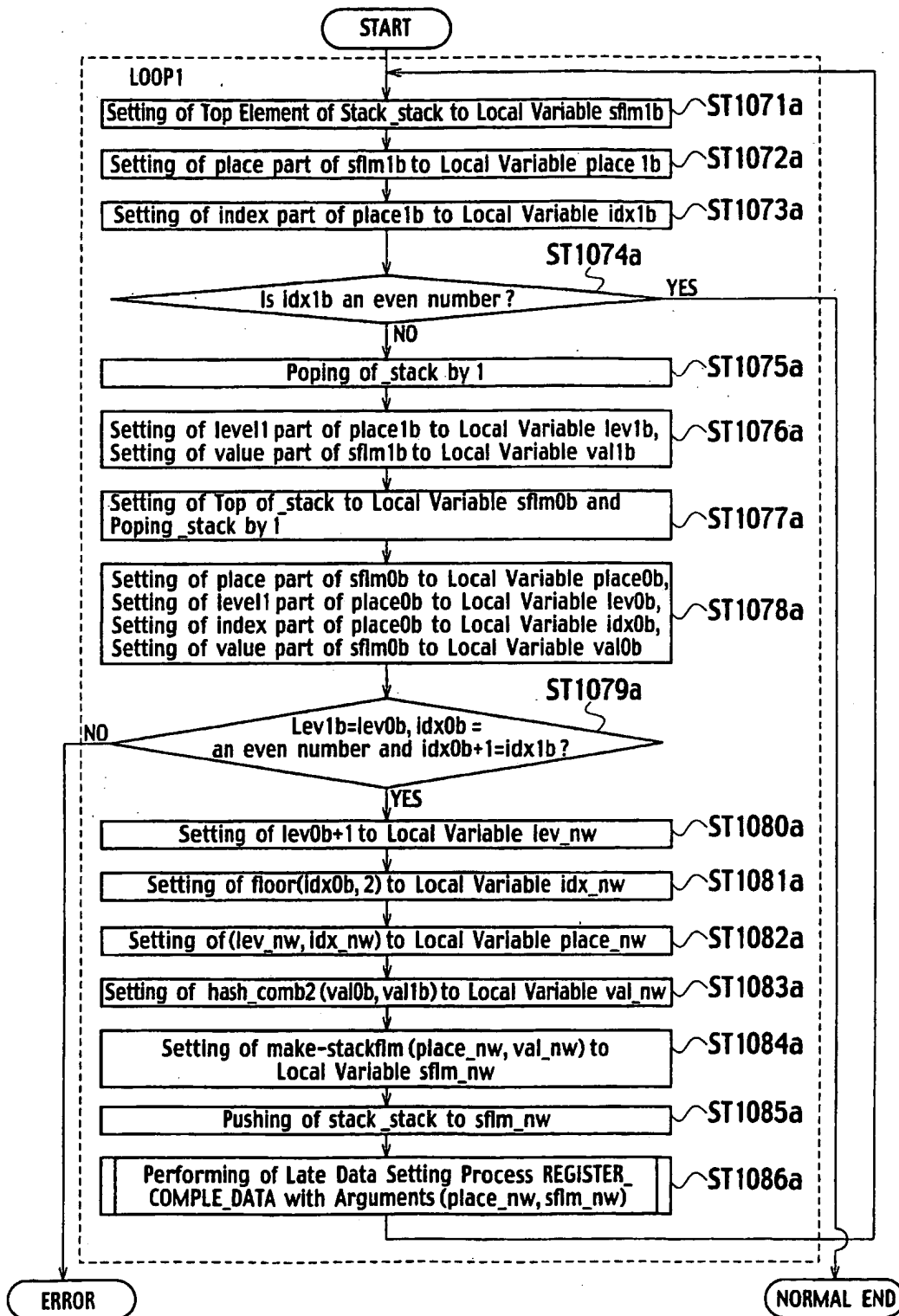


FIG. 53

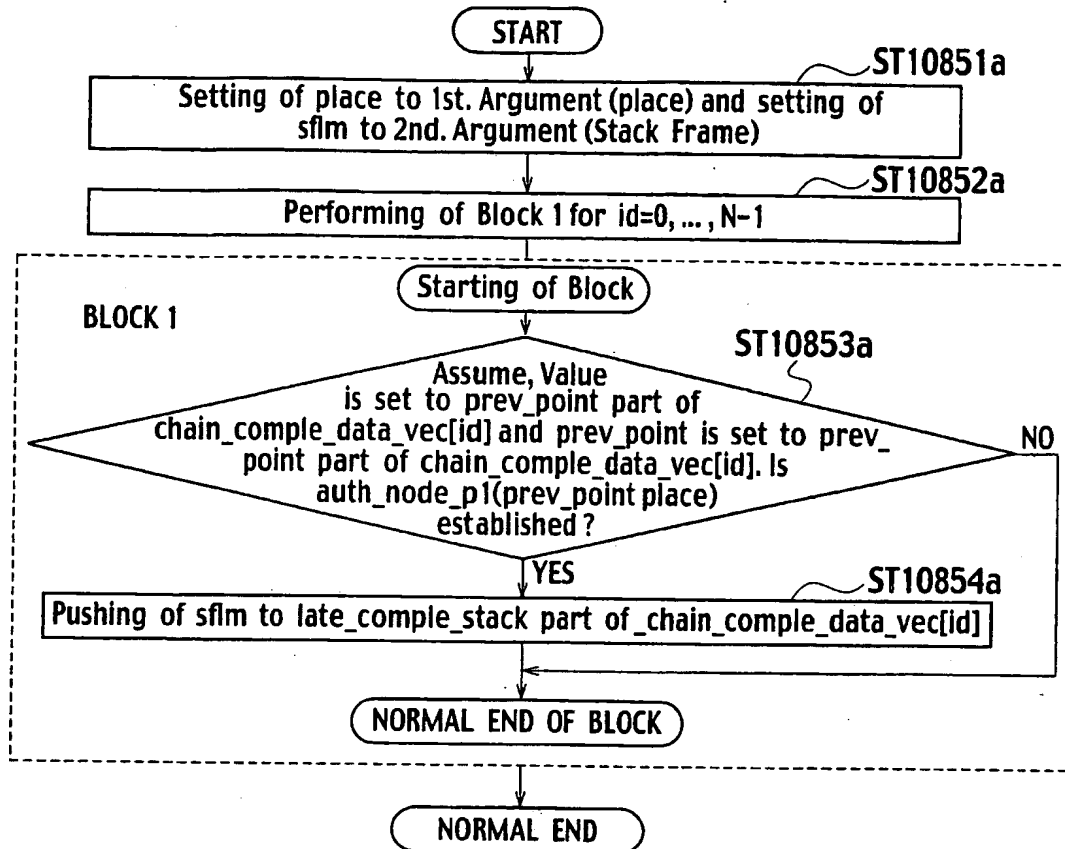


FIG. 54

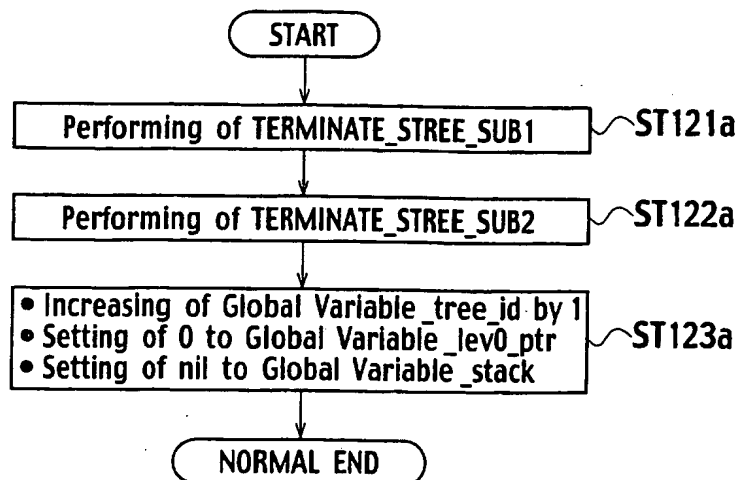


FIG. 55

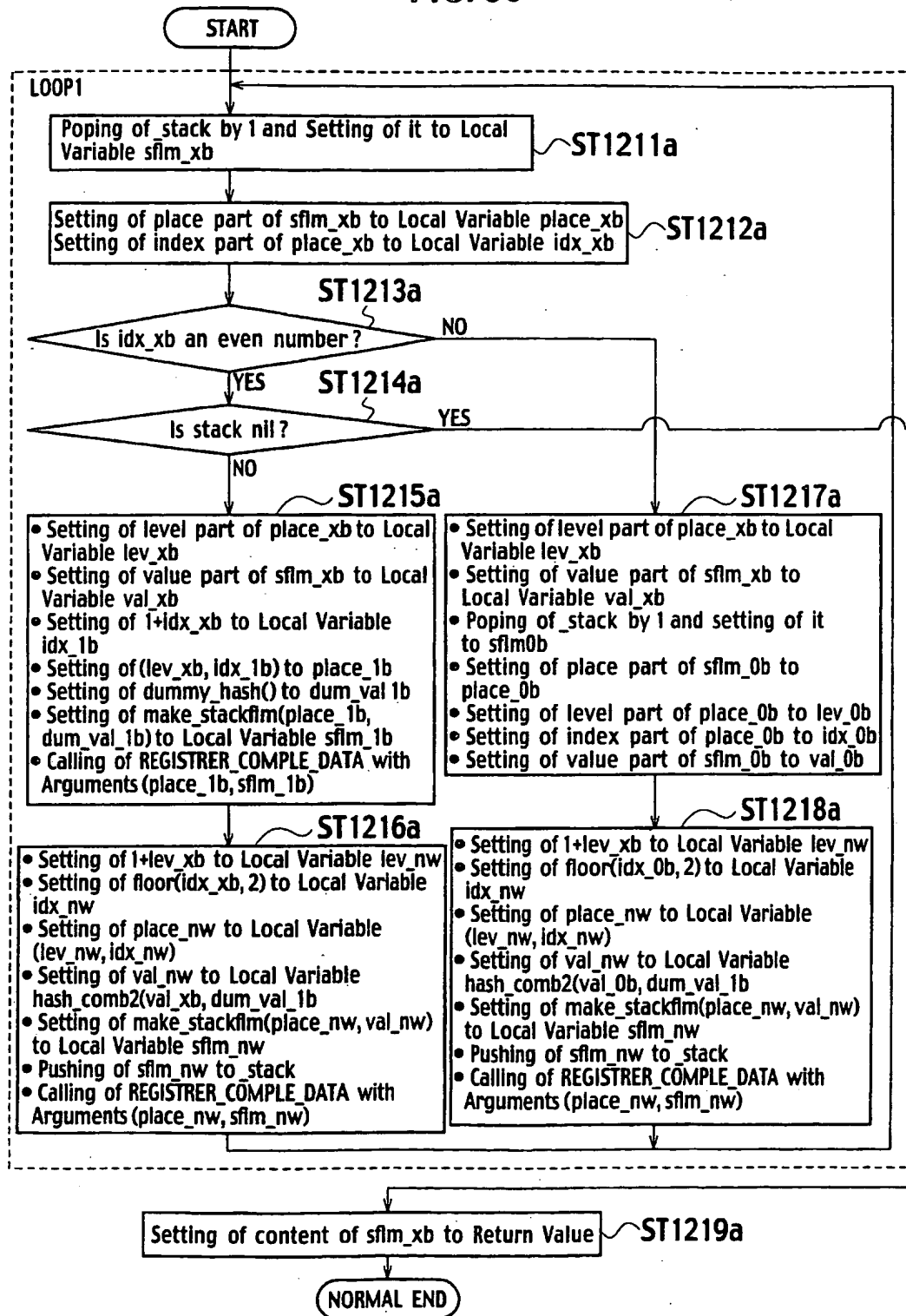


FIG. 56

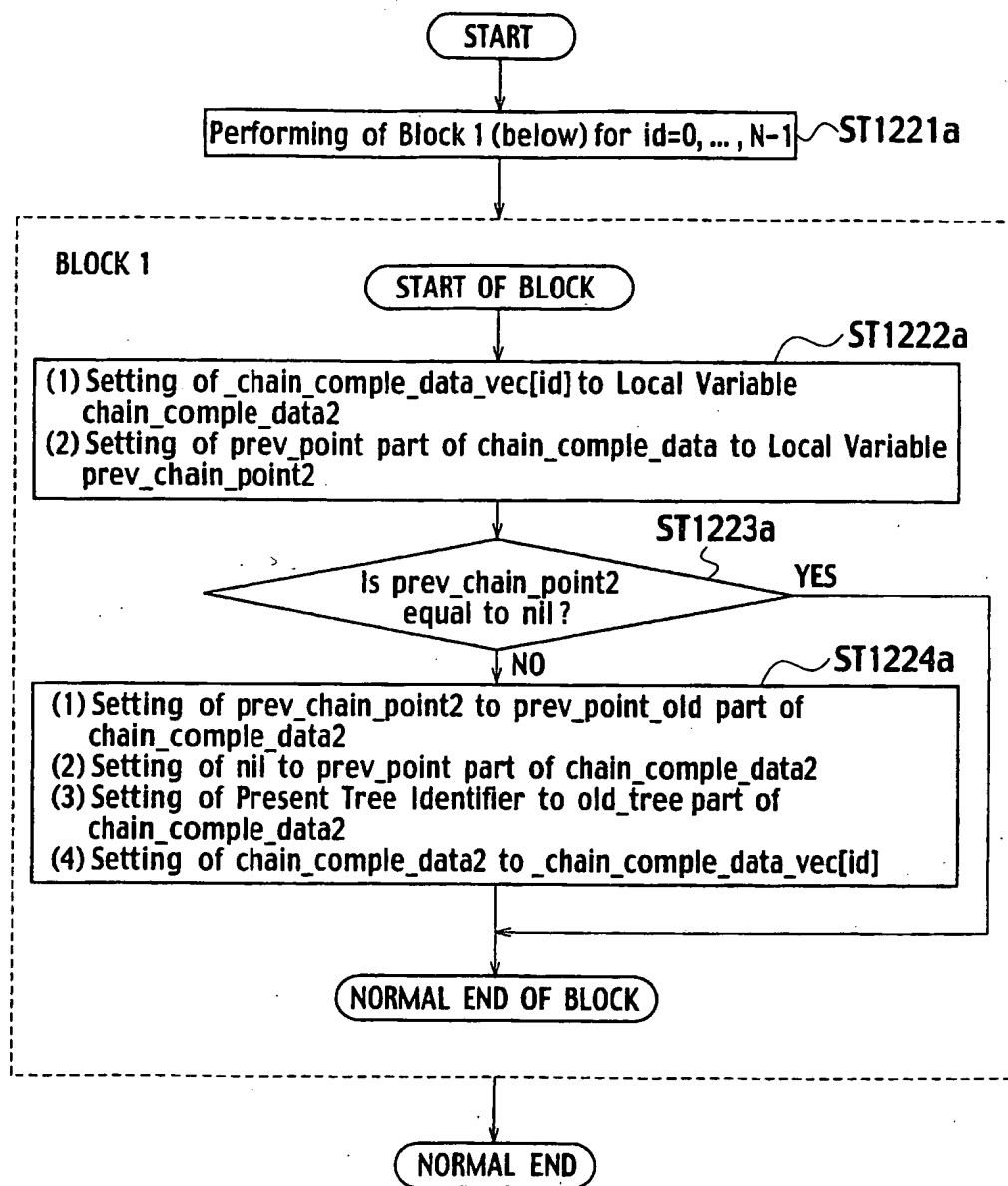


FIG. 57

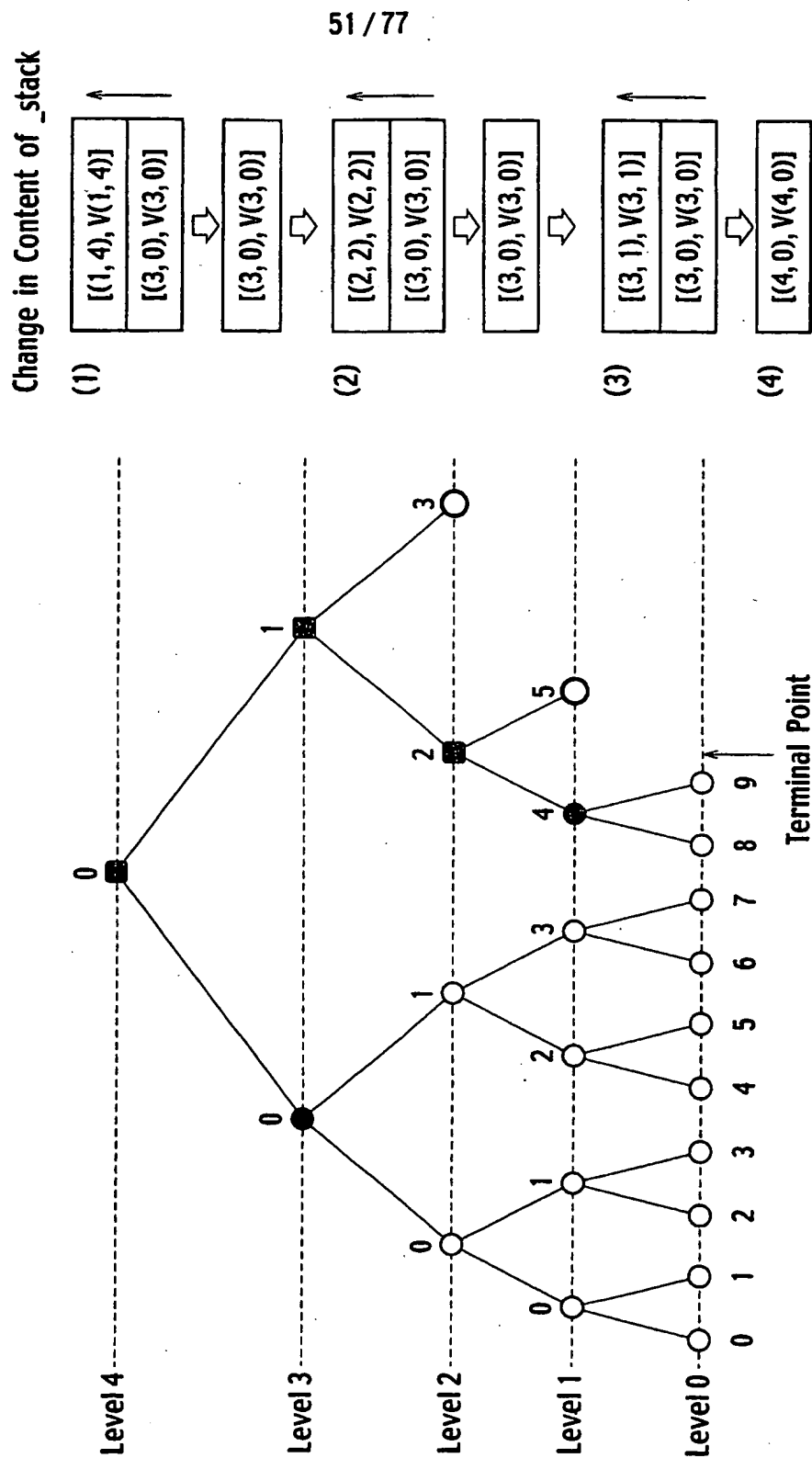
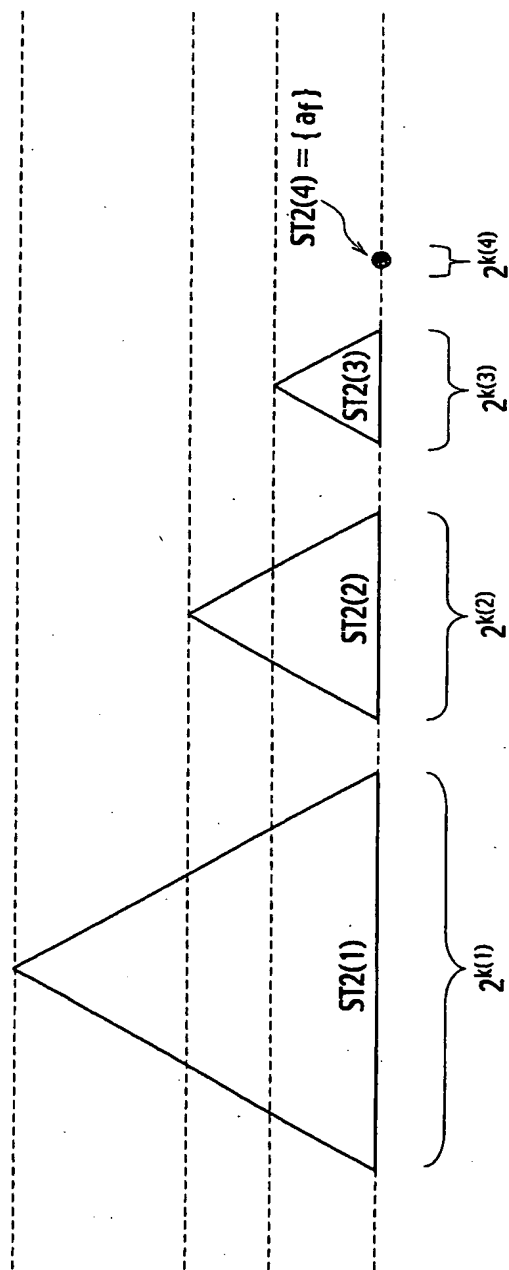
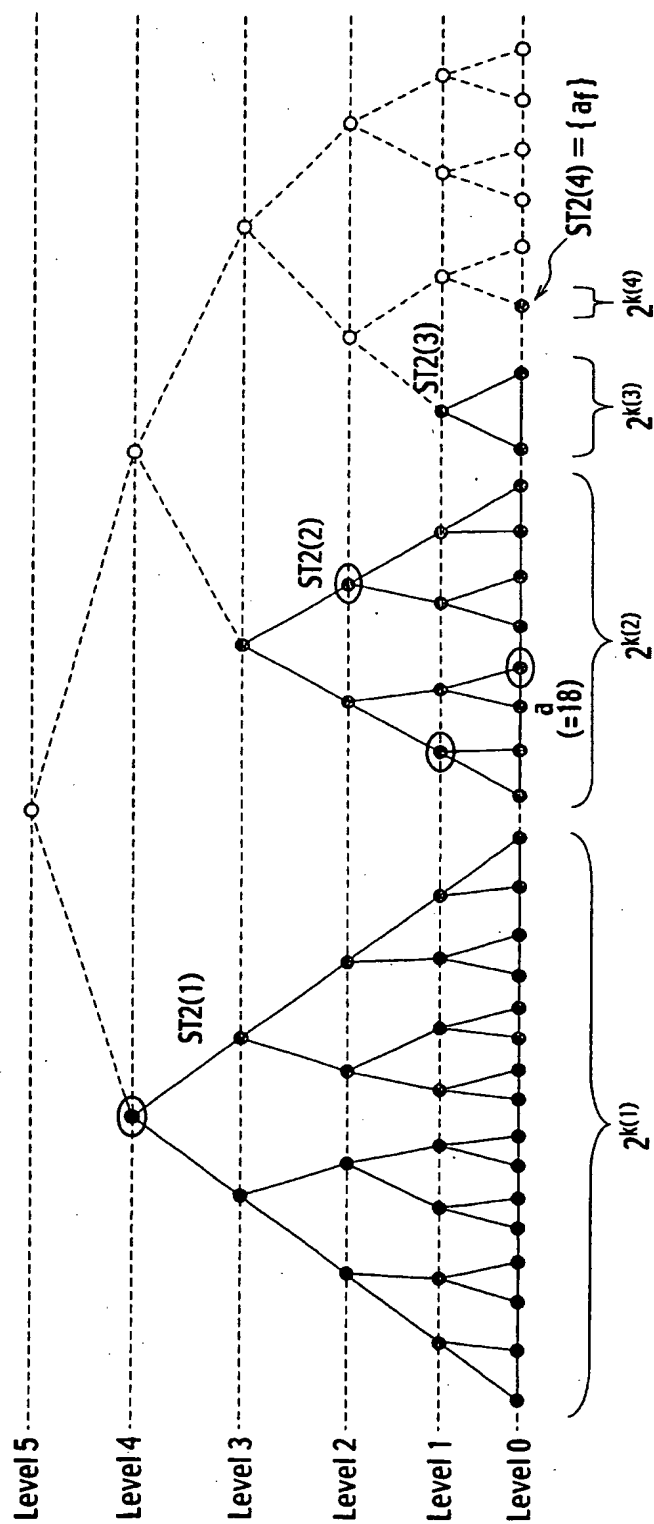


FIG. 58



$$k(1) > k(2) > k(3) > k(4) = 0$$

FIG. 59



$$k(1)=4 > k(2)=3 > k(3)=1 > k(4)=0$$

FIG. 60

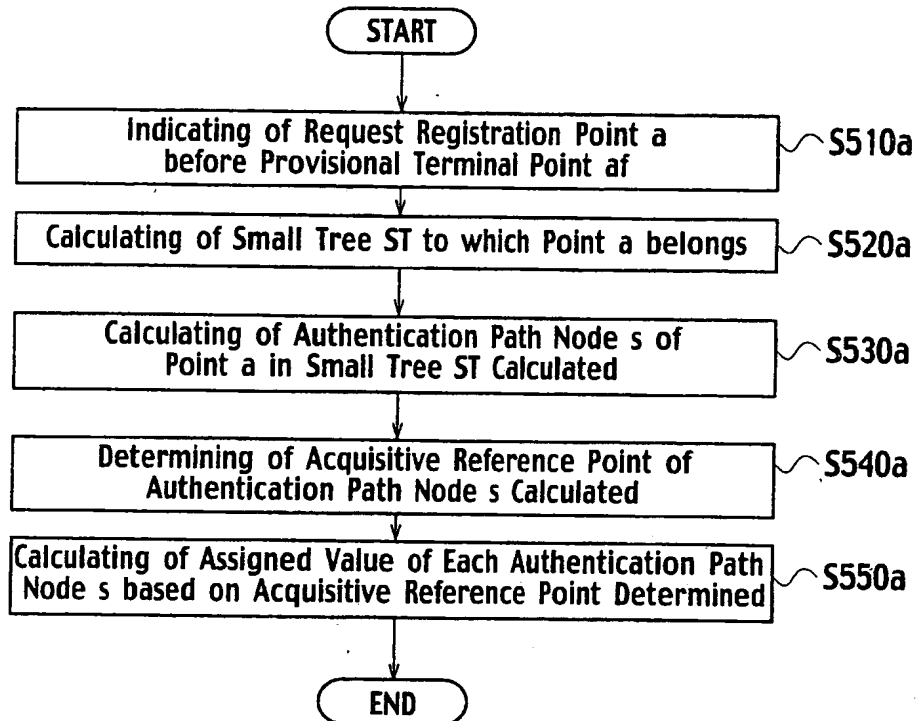
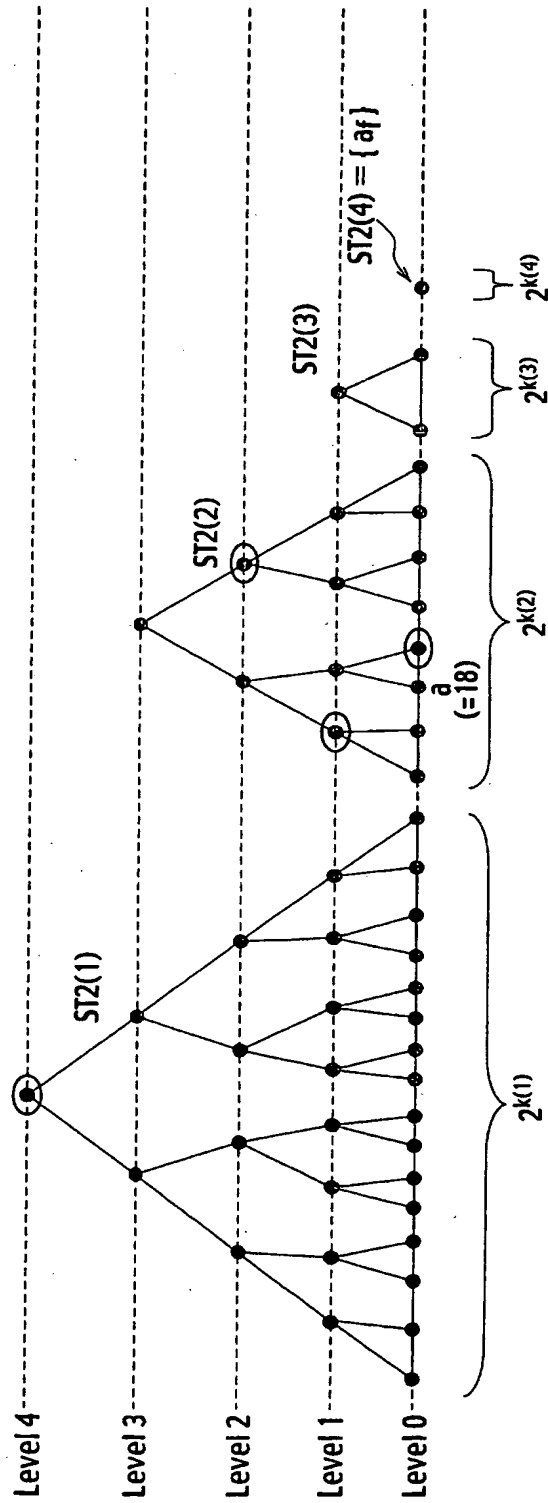


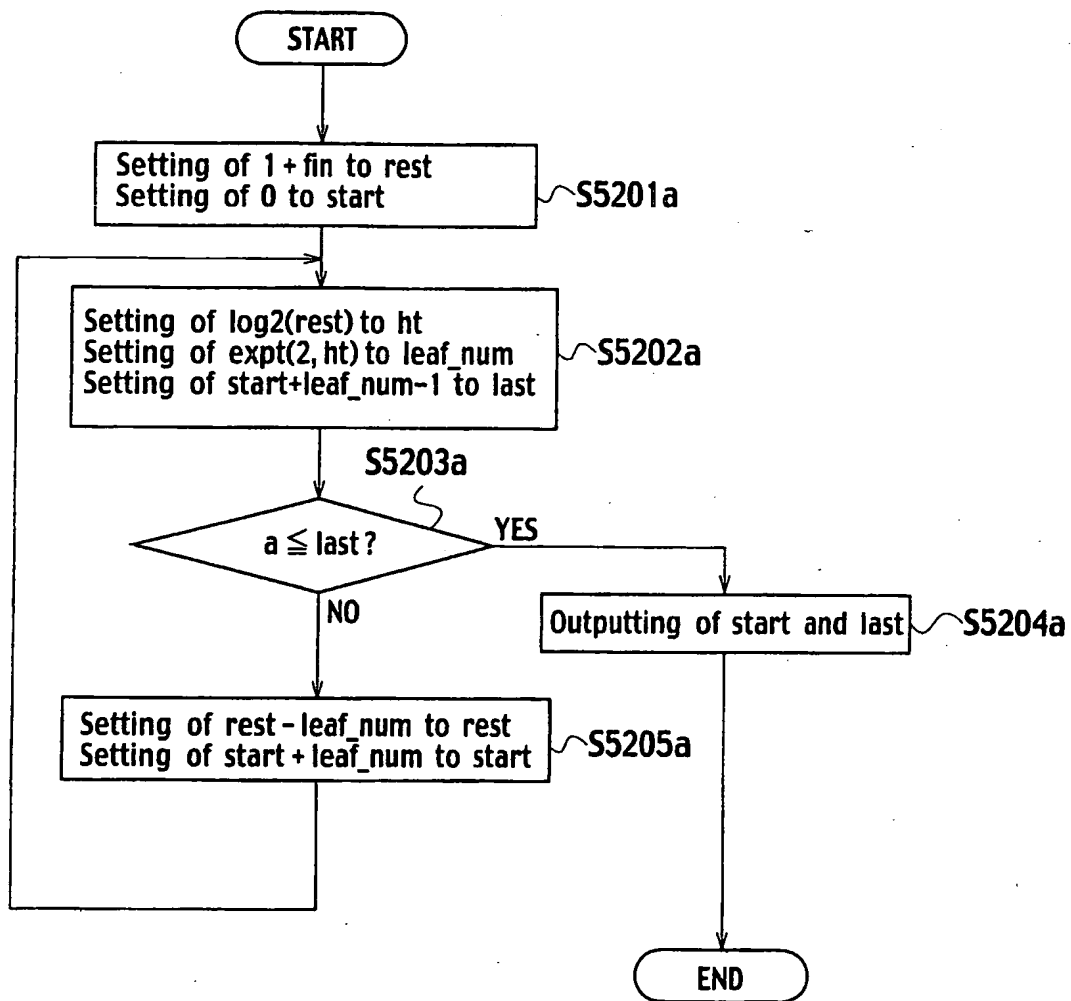


FIG. 61



$$k(1)=4 > k(2)=3 > k(3)=1 > k(4)=0$$

FIG. 62



57 / 77  
FIG. 63

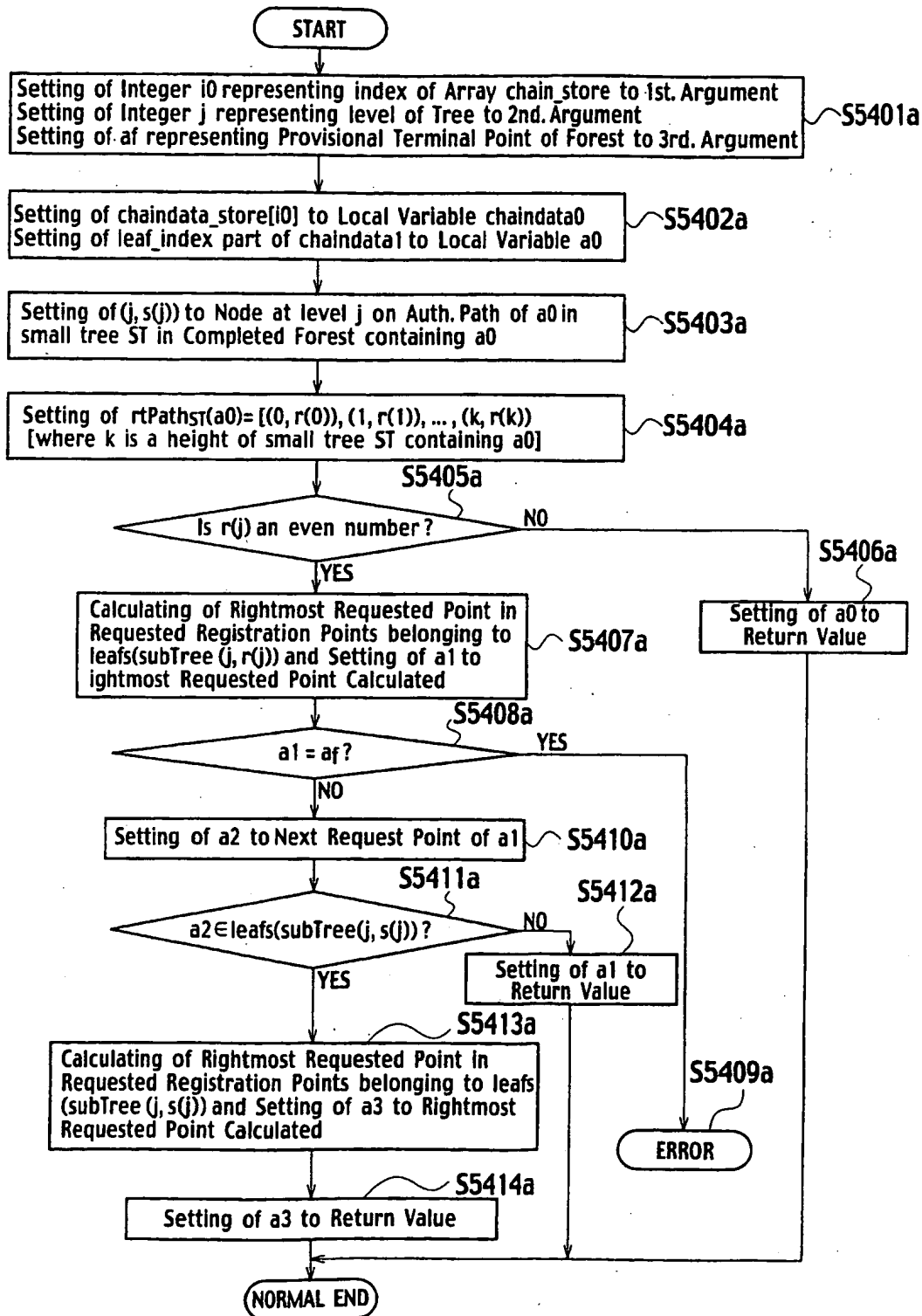


FIG. 64

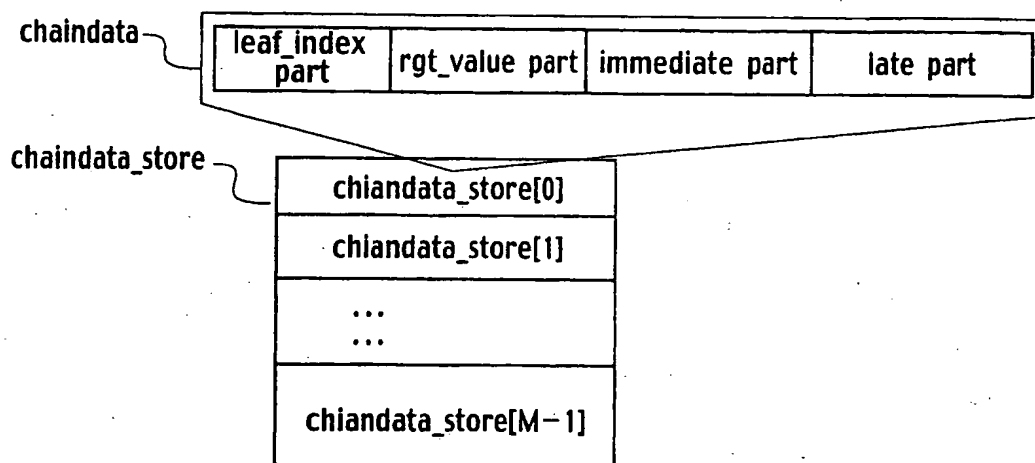


FIG. 65A

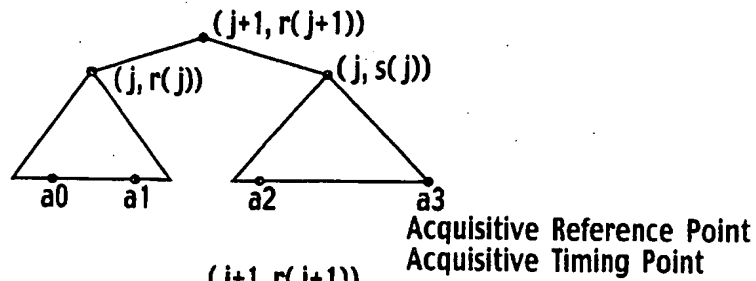


FIG. 65B

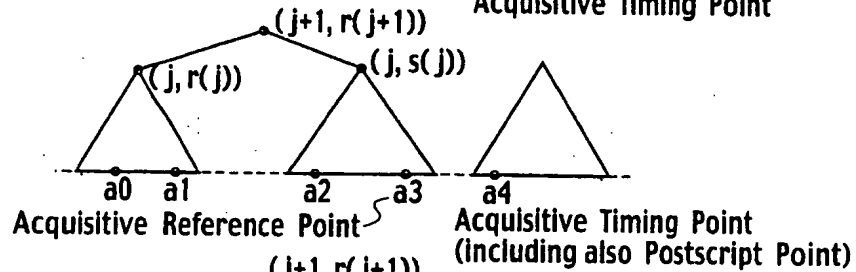


FIG. 65C

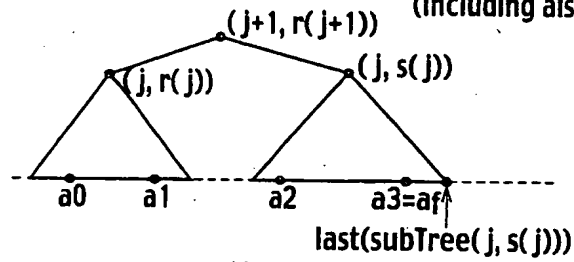


FIG. 65D

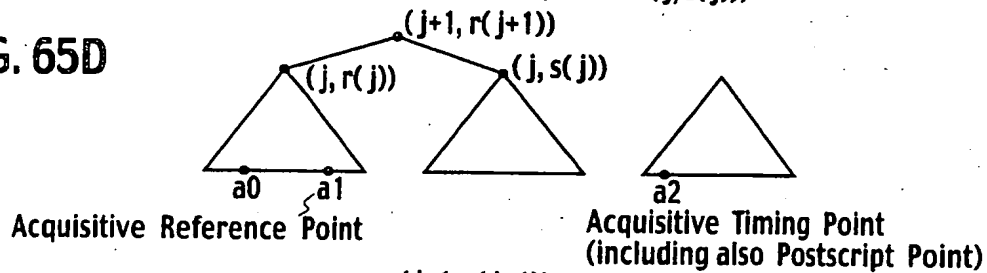


FIG. 65E

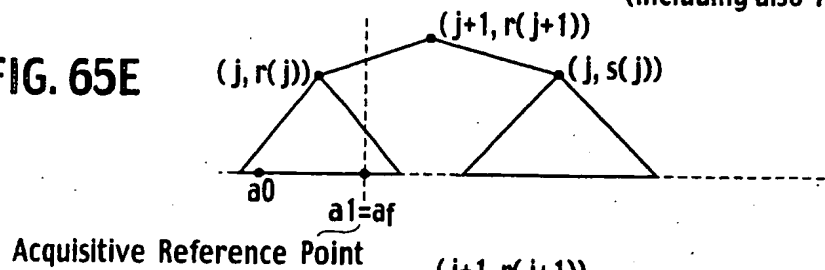
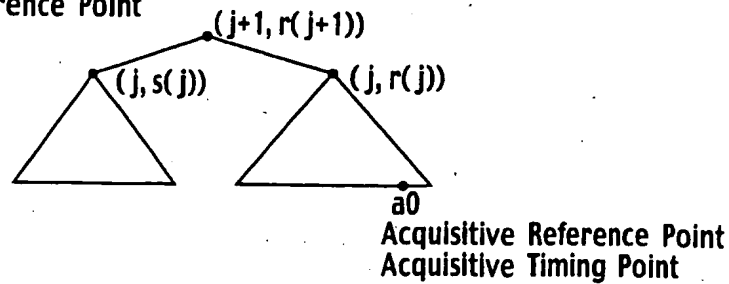


FIG. 65F



60 / 77  
FIG. 66

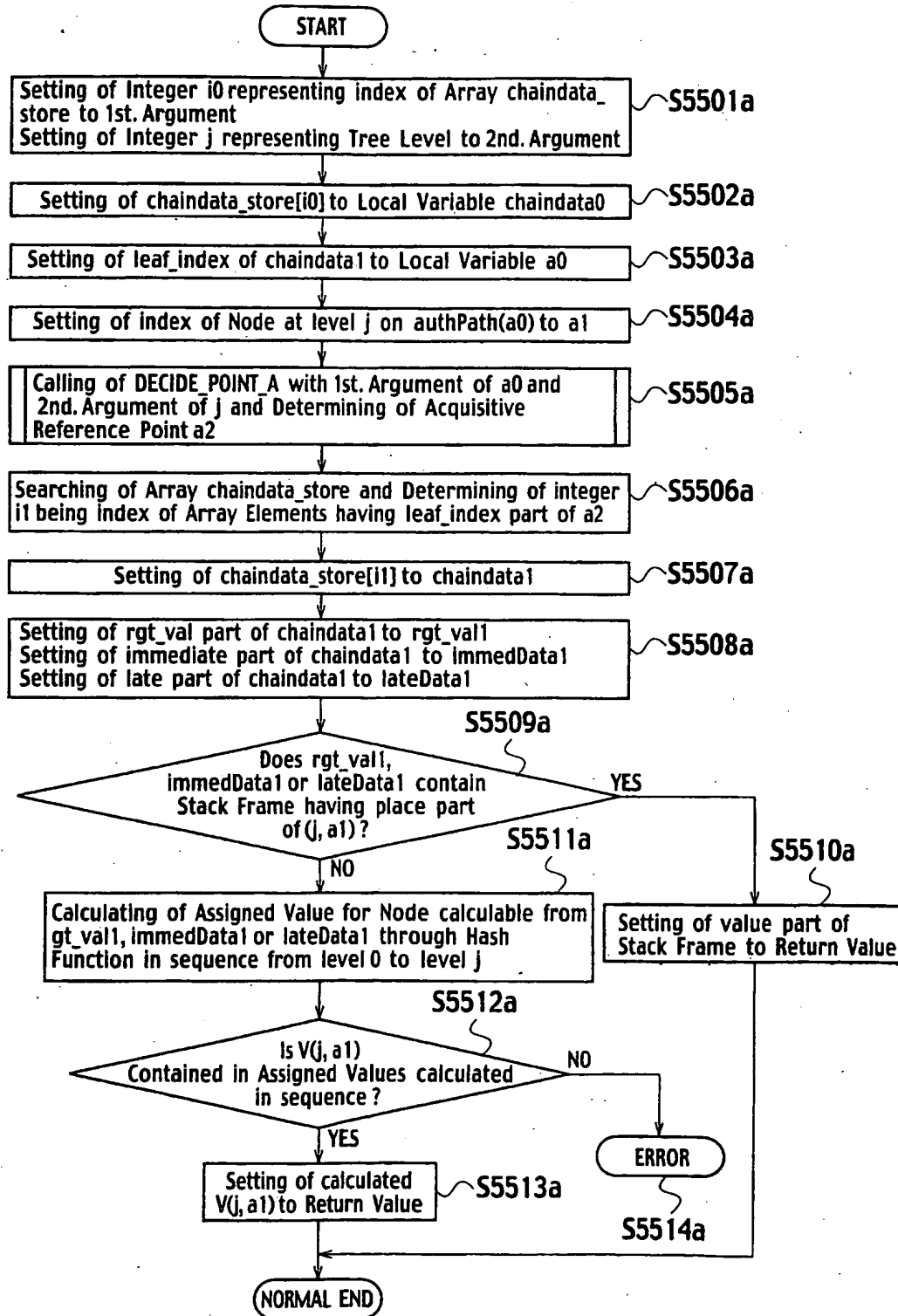
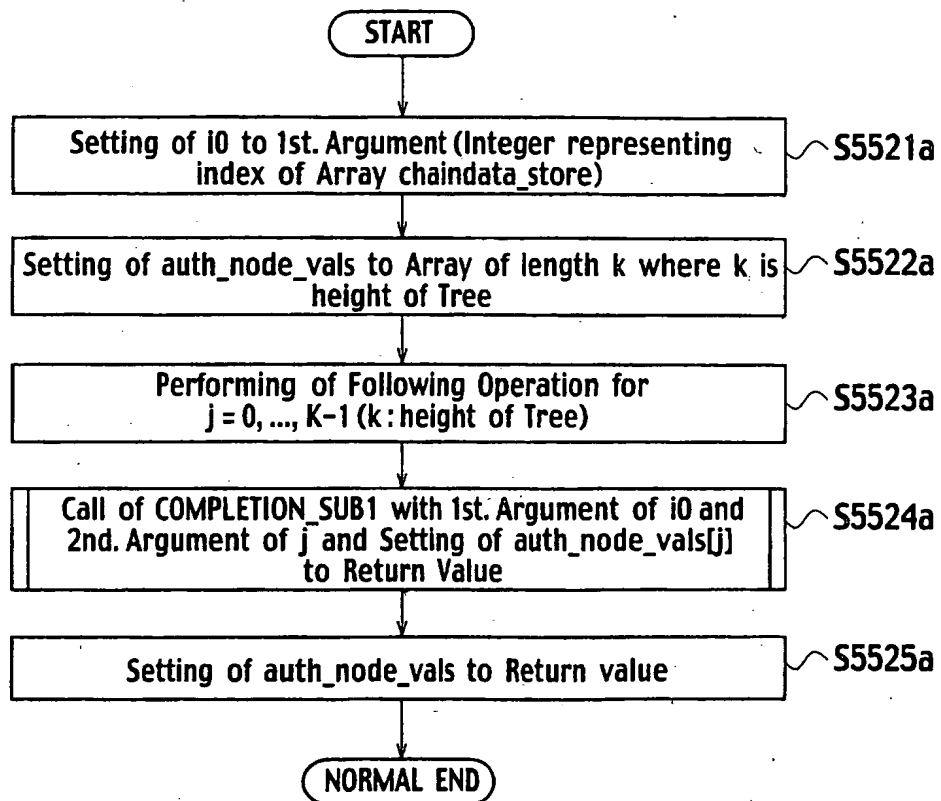


FIG. 67



62/77  
FIG. 68

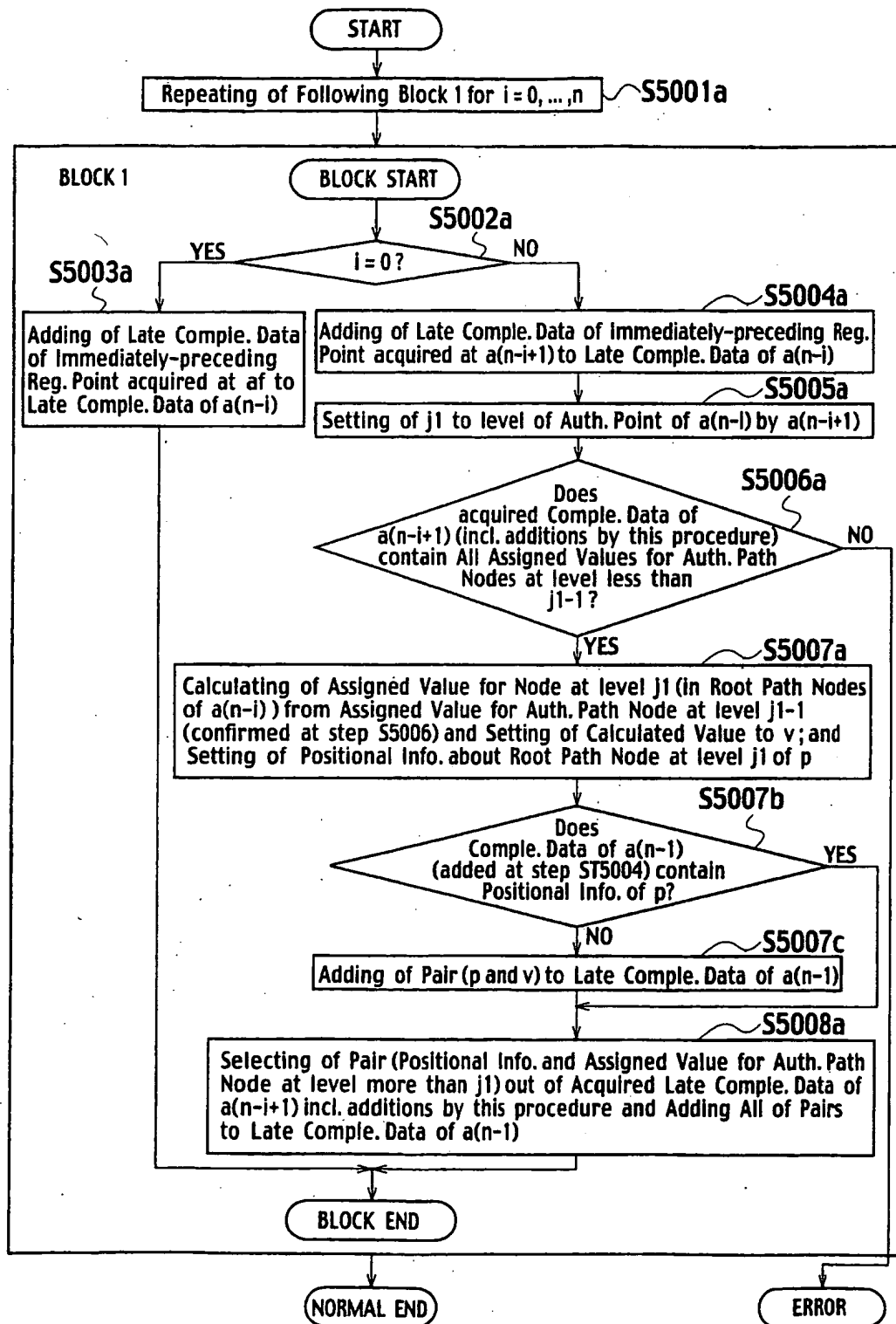




FIG. 69

Sequential Aggregation Small Tree ST2

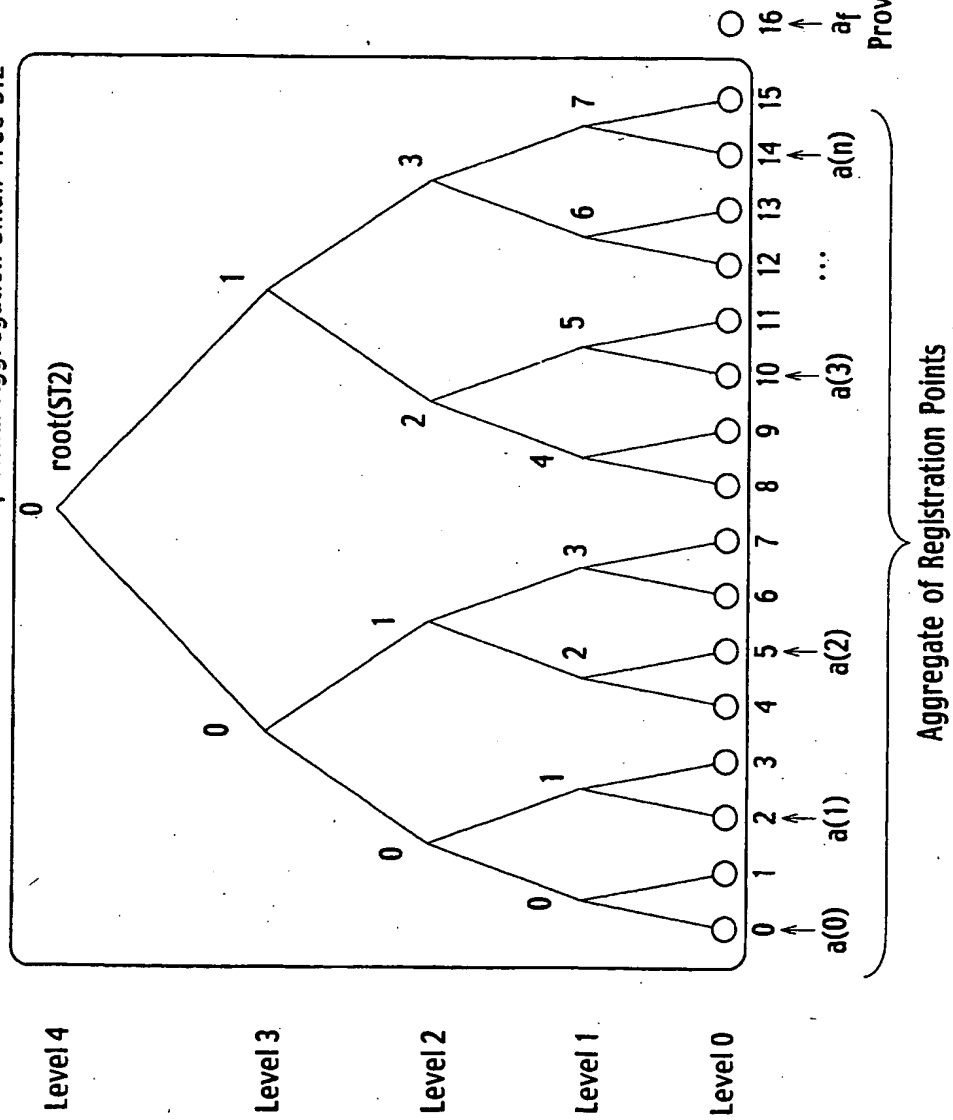


FIG. 70

Sequential Aggregation Small Tree ST2

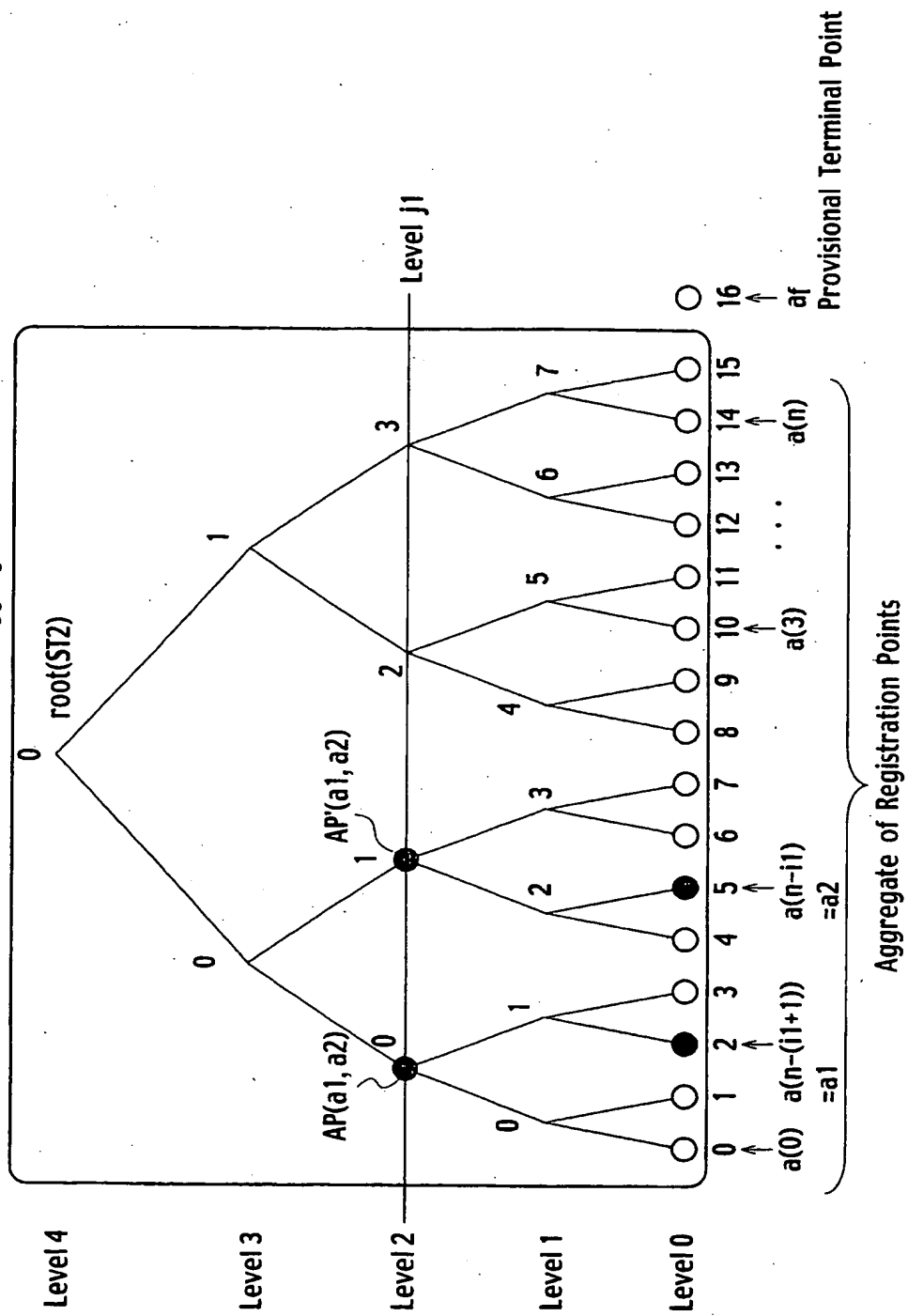
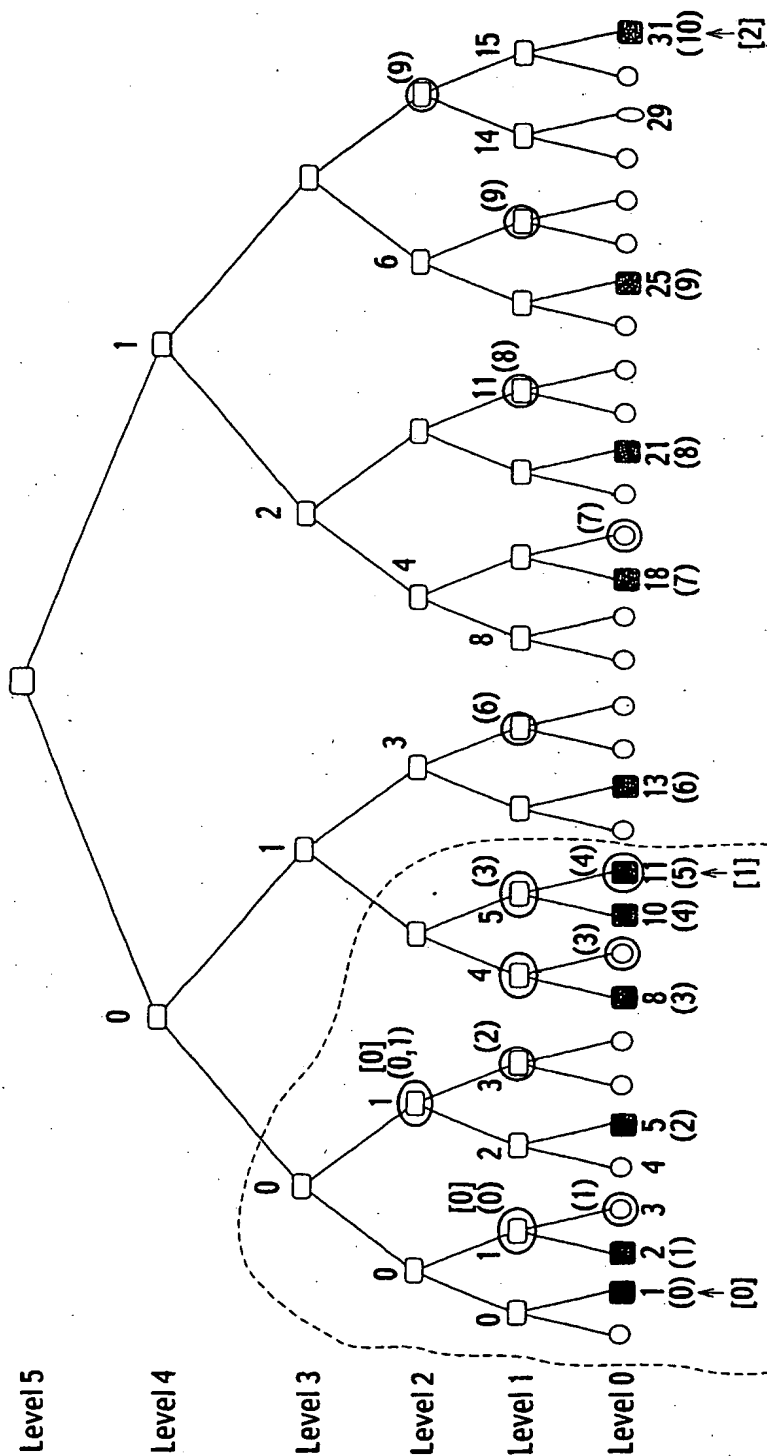




FIG. 72



Result of Local Completion for 1st. Local Data  
 Range of Original Index for Local Completion [0..5]  
 Range of Thinned-out Extraction Data Index [0..1]

FIG. 73

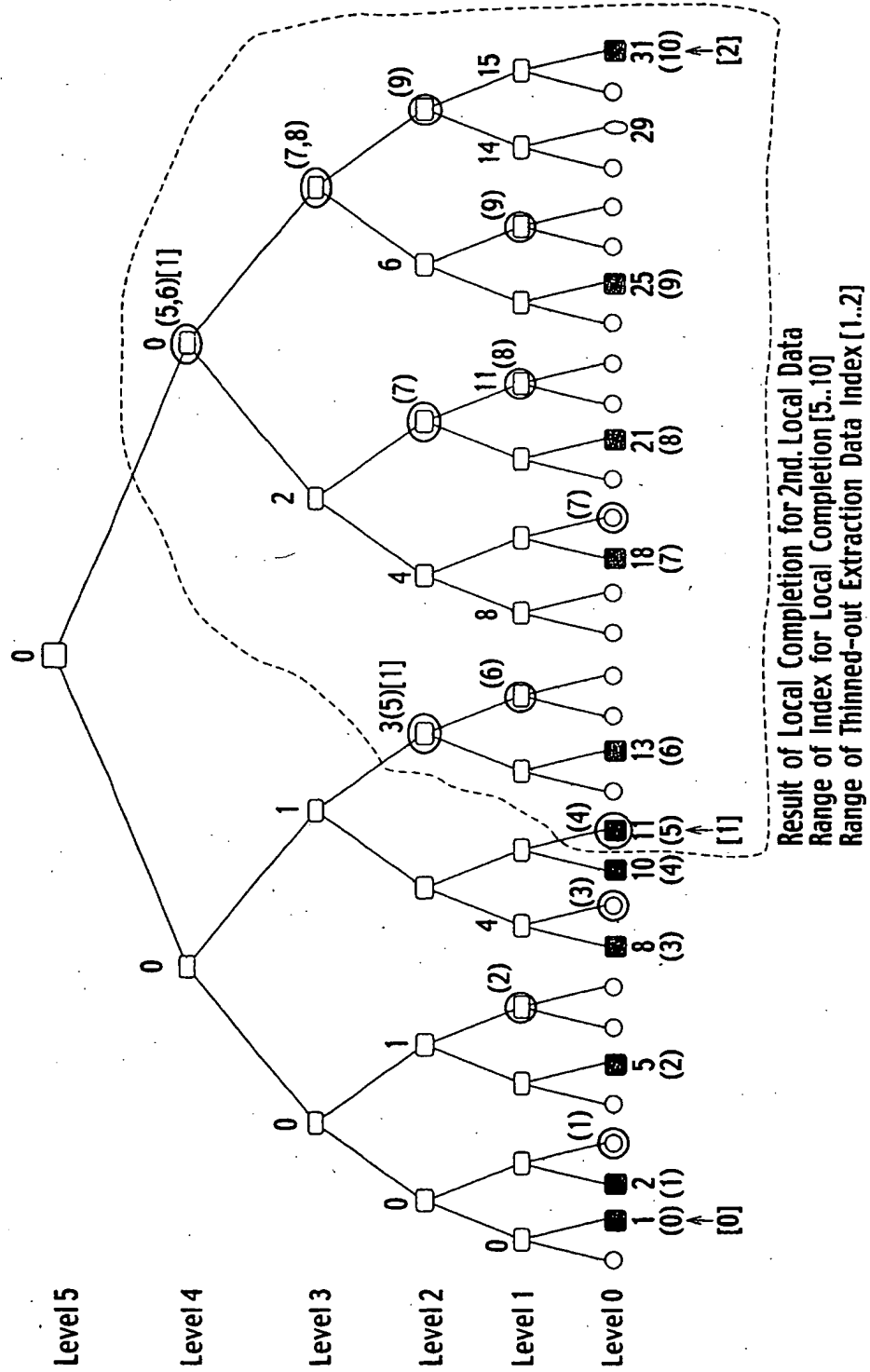


FIG. 74

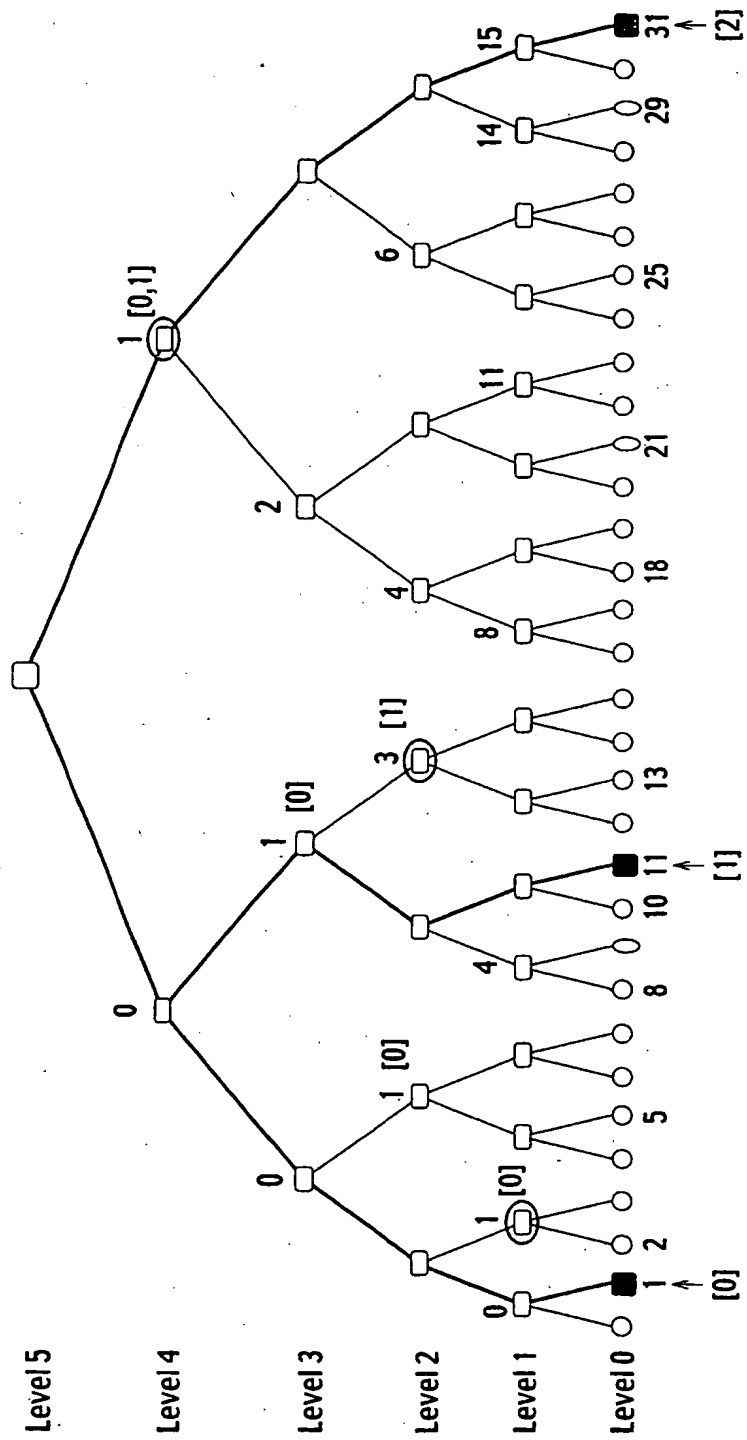


FIG. 75

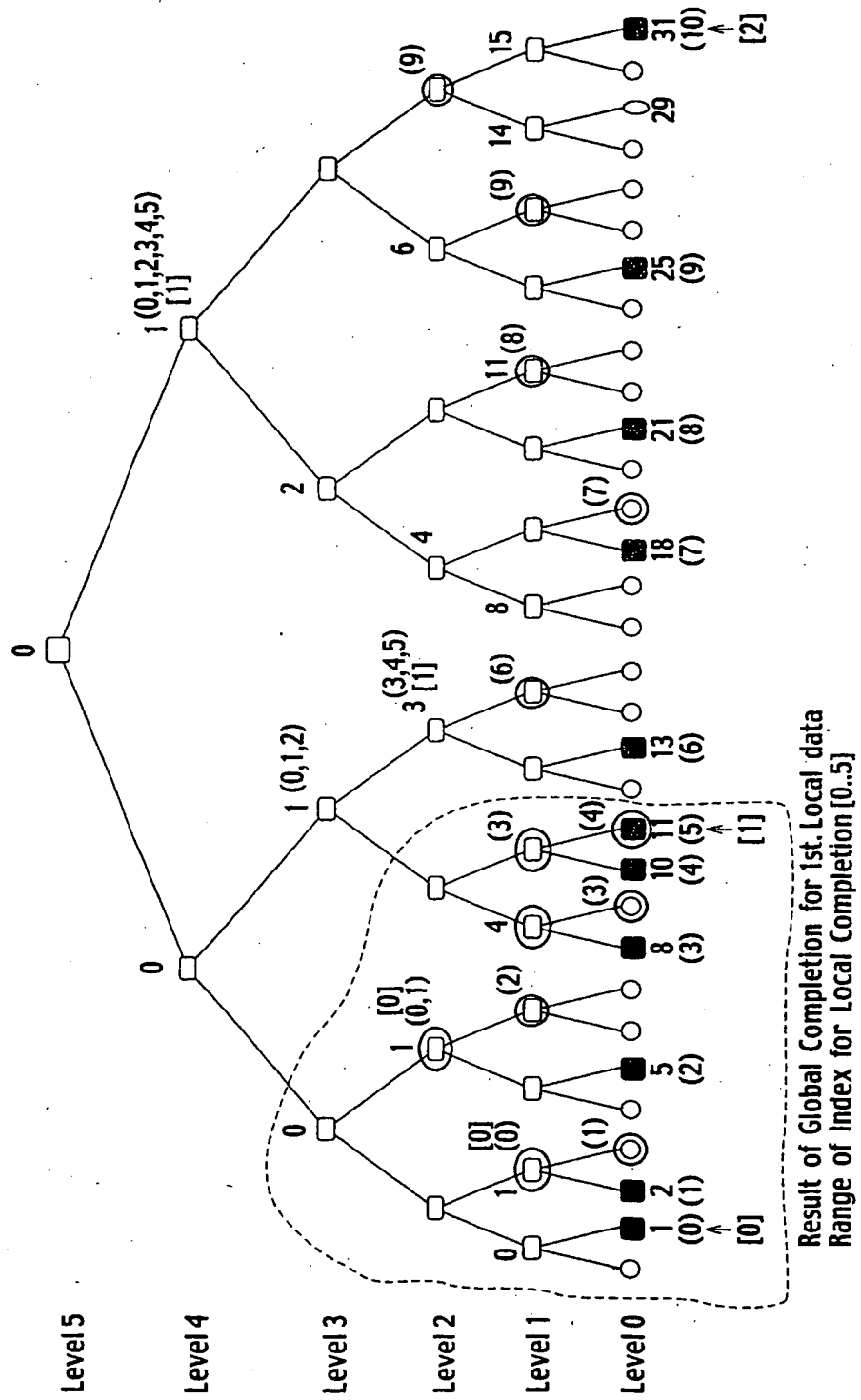


FIG. 76

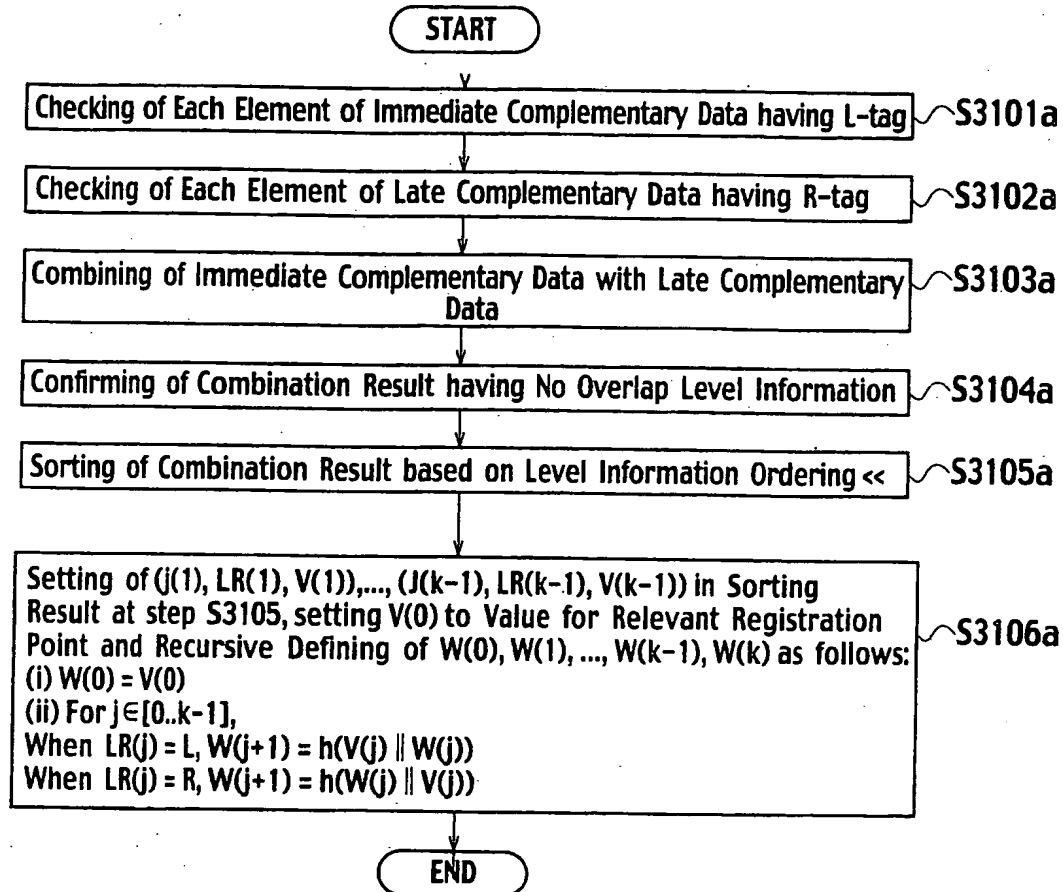


FIG. 77

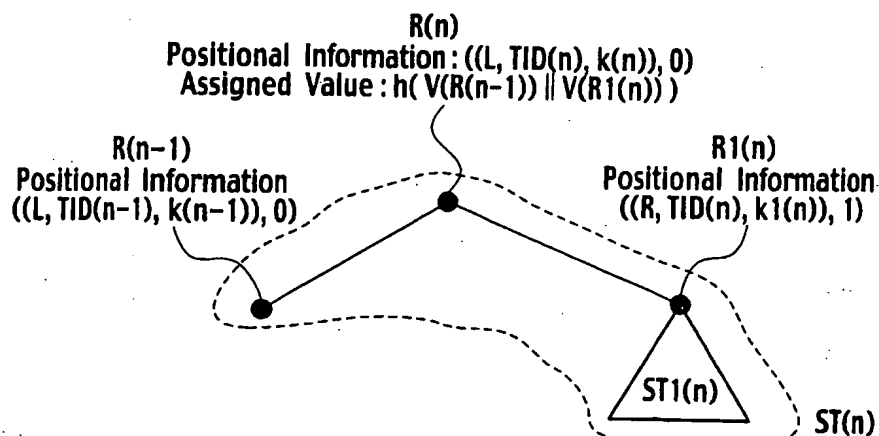
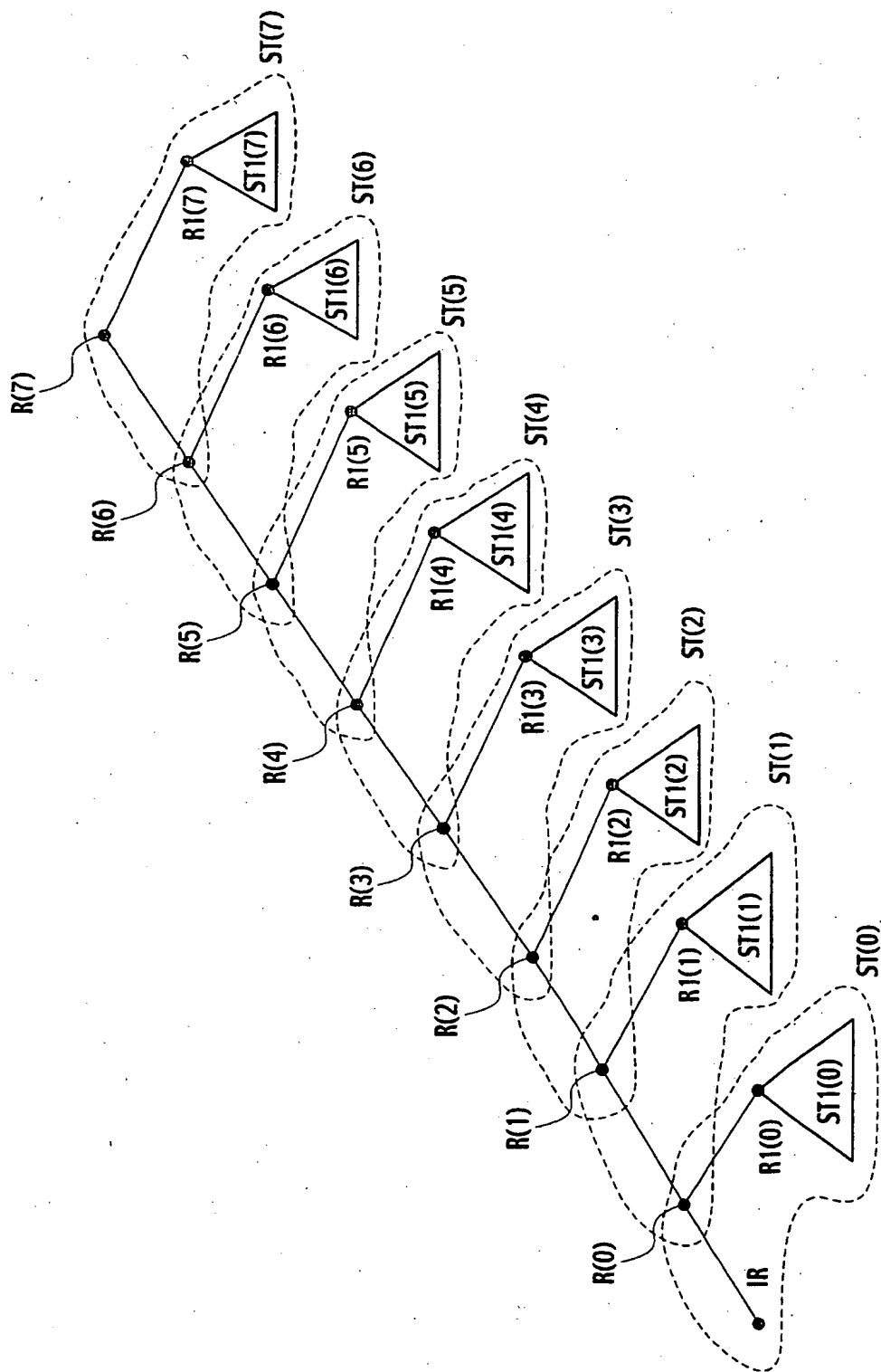
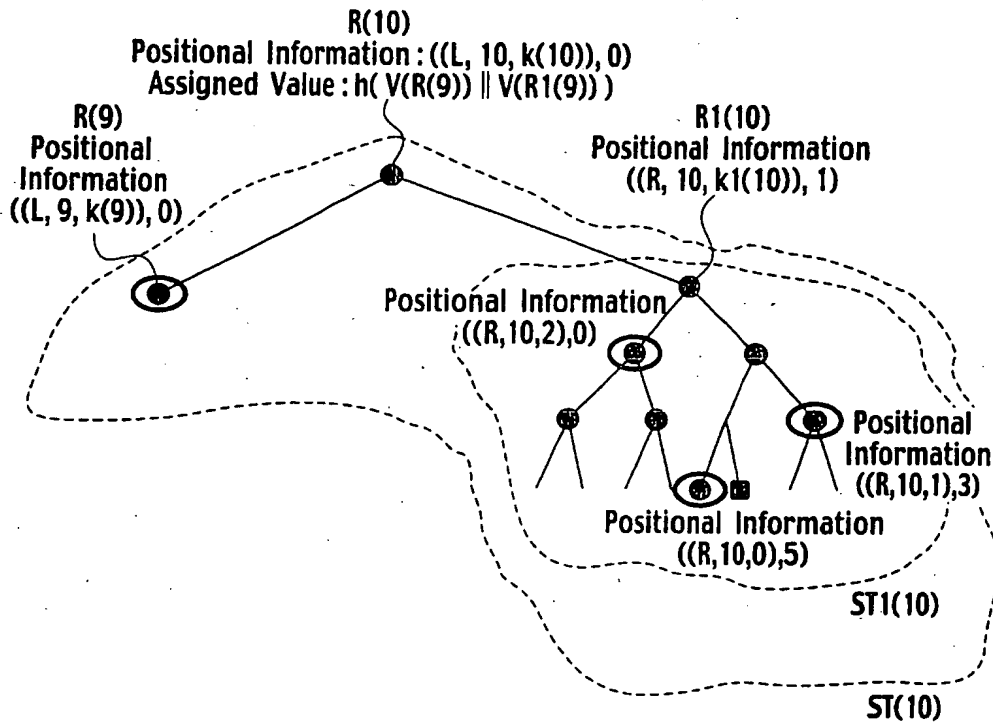




FIG. 78



72 / 77  
**FIG. 79**



**FIG. 80**

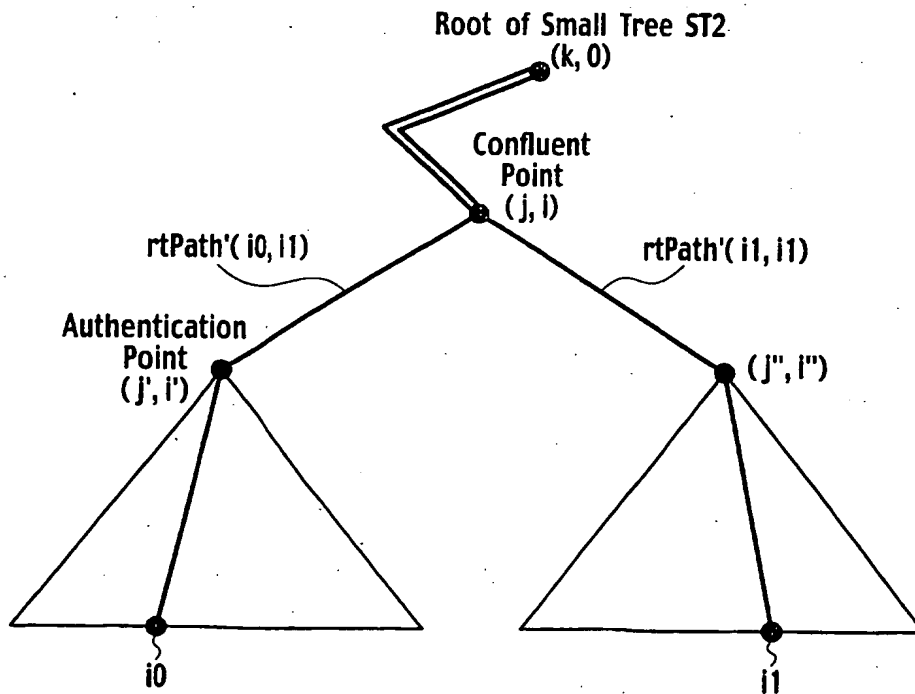




FIG. 82

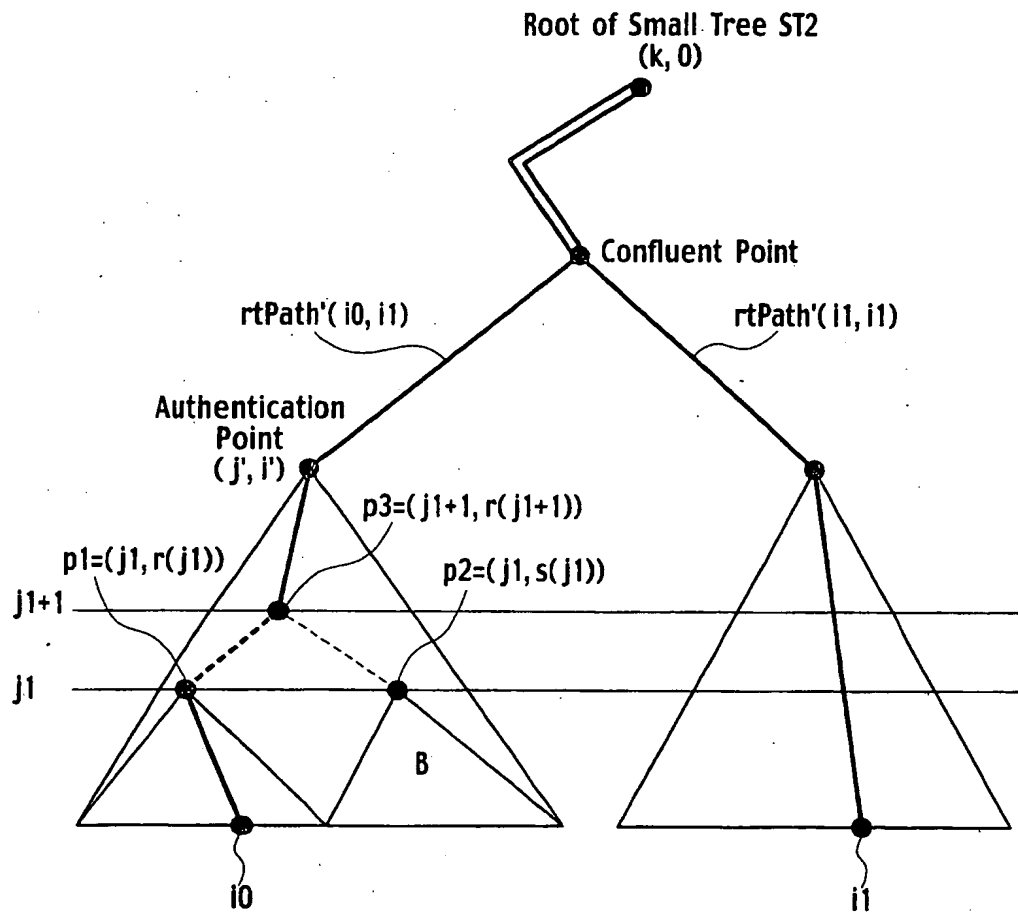


FIG. 83

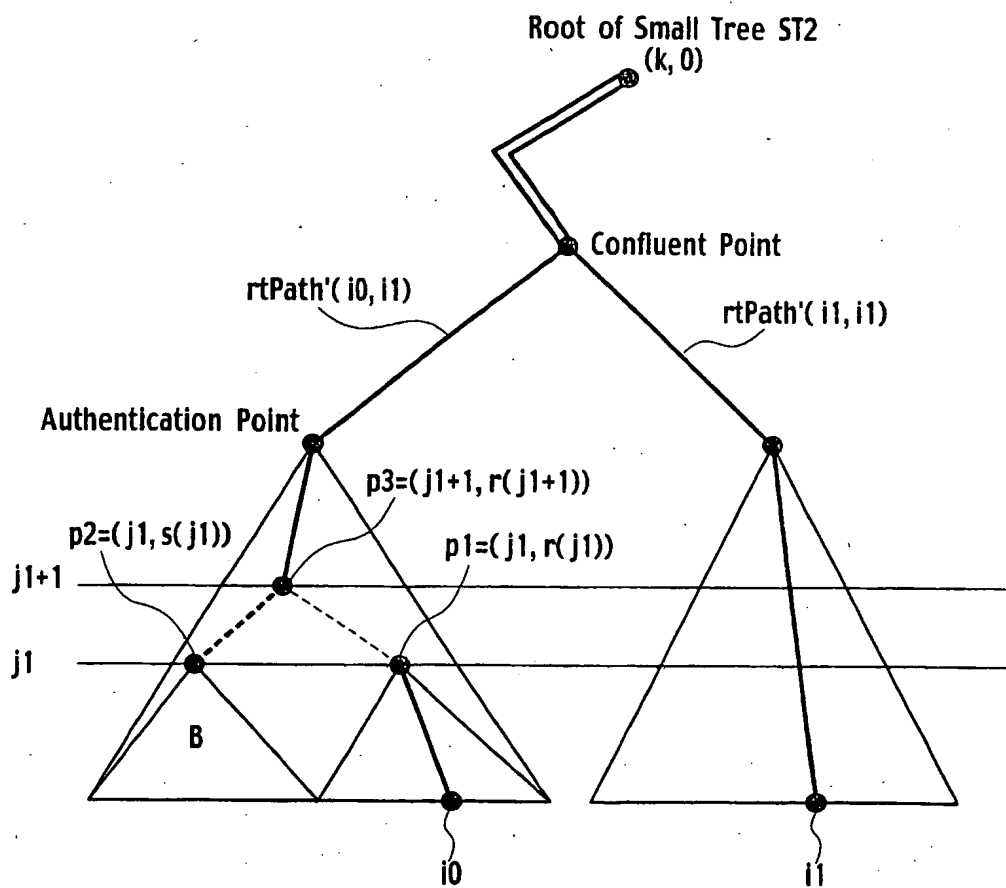
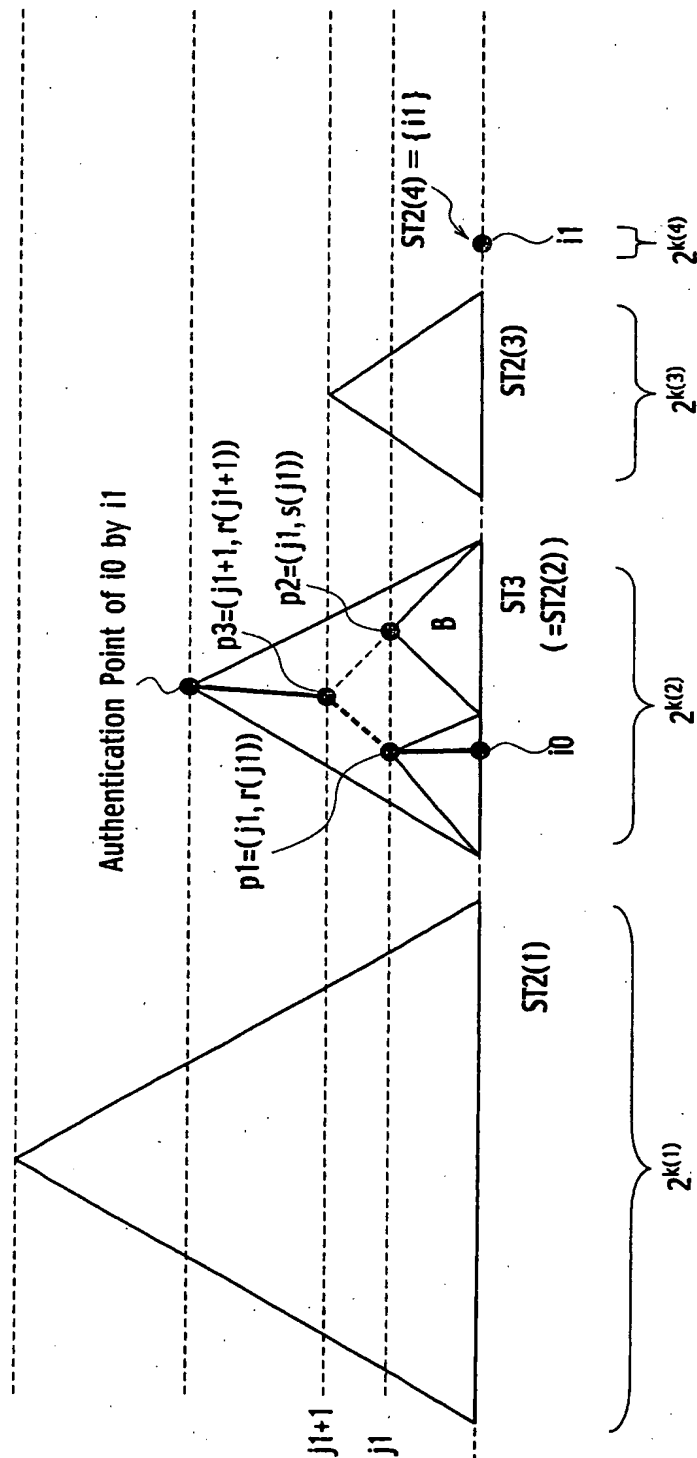
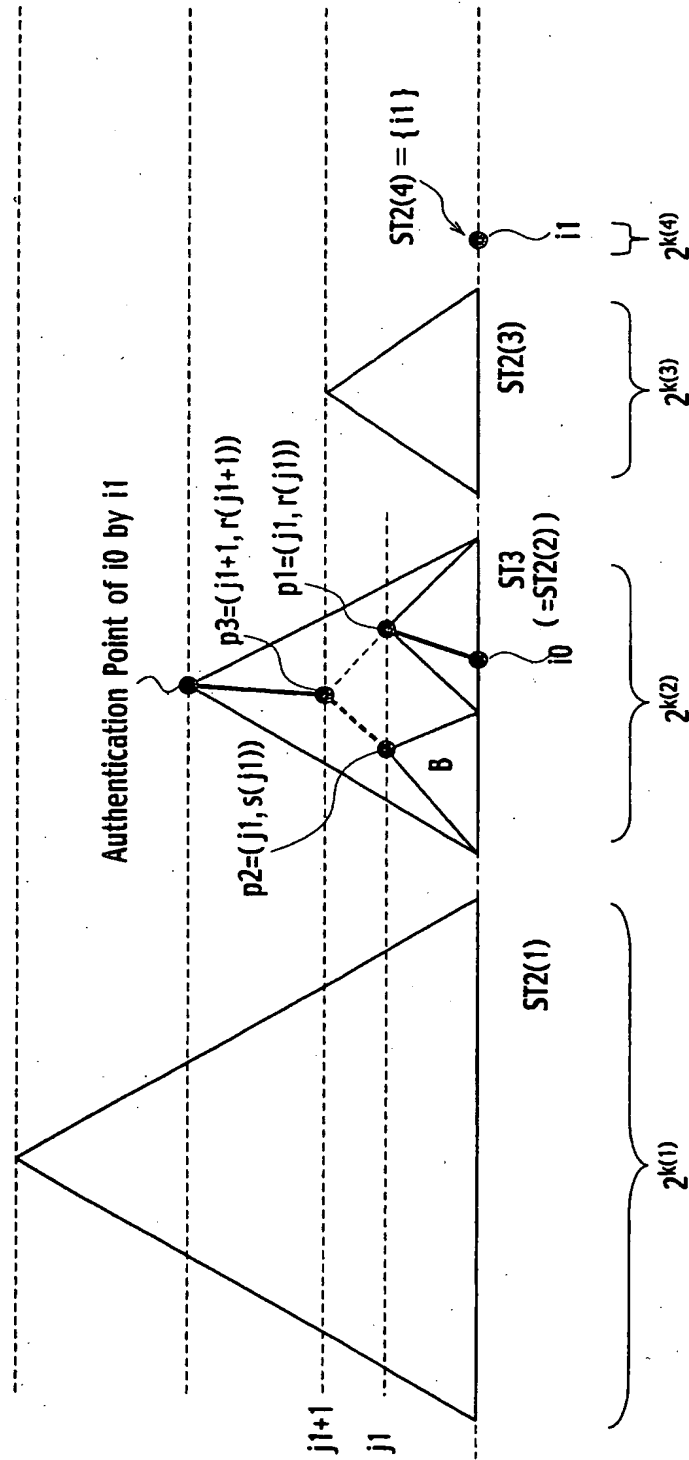


FIG. 84



$$k(1) > k(2) > k(3) > k(4) = 0$$

FIG. 85



$$k(1) > k(2) > k(3) > k(4) = 0$$

## CLAIMS

1. An event-ordering certification method for an event-ordering certification system having a user apparatus performing an event-ordering request for certifying  
5 a chronological sequence of a certain event in time-series events generating a designated digital information, a certification apparatus for drafting a certificate for the event-ordering request of the user apparatus, an audit apparatus for auditing authenticity of the certificate and a communication network for connecting the user apparatus, the certification apparatus and the audit apparatus with each other,  
10 the method comprising:
  - an event-ordering request receiving step where the certification apparatus receives the event-ordering request from the user apparatus;
  - a sequentially assigned data-item calculating step where the certification apparatus drafts a sequentially assigned data-item from the digital information  
15 included in the event-ordering request in accordance with a predetermined procedure;
  - an event-ordering request aggregating step where, in sequential aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a  
20 directed tree from left thereof, the certification apparatus calculates assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash  
25 function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;
  - a certificate drafting step where the certification apparatus drafts a certificate containing the sequentially assigned data-item and a first sequential aggregation tree specifying information for specifying the sequential aggregation  
30 tree and a leaf thereof both having the sequentially assigned data-item assigned



thereto;

a certificate sending step where the certification apparatus sends the certificate to the user apparatus;

assuming that: a leaf of the sequential aggregation tree to which the event-ordering request is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the certificate; and in the complementary information, a complementary information acquirable at a point of assigning the event-ordering request to the sequential aggregation tree is defined as an immediate complementary information,

an audit certificate drafting step where after assigning the event-ordering request to the sequential aggregation tree, the certification apparatus assigns a first audit request to the sequential aggregation tree thereby drafting a first audit certificate in the same way as drafting the certificate, acquires a first immediate complementary information for audit at the point of assigning the first audit request to the sequential aggregation tree, from the sequential aggregation tree and incorporates the first immediate complementary information into the first audit certificate;

an audit certificate sending step where the certification apparatus sends the first audit certificate to the audit apparatus;

a complementary information request receiving step where after assigning the first audit request to the sequential aggregation tree, the certification apparatus receives a request of the complementary information of the certificate from the user apparatus;

a late complementary information drafting step where the certification apparatus acquires a second sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the request of the complementary information assigned thereto and a complementary information acquirable at the point of assigning the request of the complementary information, from the sequential aggregation tree, thereby forming a late

complementary information; and

a late complementary information sending step where the certification apparatus sends the late complementary information about the certificate to the user apparatus.

5

2. The event-ordering certification method of claim 1, wherein at the certificate drafting step, the certification apparatus incorporates the immediate complementary information of the certificate into the first sequential aggregation tree specifying information.

10

3. The event-ordering certification method of claim 1 or 2, wherein:

the audit certificate drafting step further includes a step where before assigning the event-ordering request to the sequential aggregation tree, the certification apparatus assigns a second audit request to the sequential aggregation tree thereby drafting a second audit certificate in the same way as drafting the certificate, acquires a second immediate complementary information for audit at the point of assigning the second audit request to the sequential aggregation tree, from the sequential aggregation tree and incorporates the second immediate complementary information into the second audit certificate; the event-ordering certification method further comprising:

15

an audit late complementary information drafting step where after completing the regular time interval, the certification apparatus acquires all of the complementary information about the first and second audit certificates drafted at the audit certificate drafting step, from the sequential aggregation tree thereby forming a late complementary information about the first and second audit certificates; and

20

an audit late complementary information sending step where the certification apparatus sends the late complementary information about the first and second audit certificates to the audit apparatus.

25  
30

4. The event-ordering certification method of any one of claims 1 to 3, wherein at the sequentially assigned data-item calculating step, the sequentially assigned data-item calculated by the certification apparatus comprises a result value obtained by applying a designated collision-resistant hash function on the digital information contained in the event-ordering request.

5. The event-ordering certification method of any one of claims 1 to 4, wherein at the certificate drafting step, the certification apparatus applies a digital signature on the certificate drafted.

6. The event-ordering certification method of any one of claims 1 to 5, further comprising an electronic information publishing step where the certification apparatus electronically publishes the root value of the sequential aggregation tree after completing the regular time interval.

7. The event-ordering certification method of any one of claims 1 to 6, wherein for a plurality of event-ordering requests from the user apparatus, the certificate sending step further includes a step where the certification apparatus sends respective certificates for the event-ordering requests in chronological sequence of assigning the event-ordering requests to the sequential aggregation tree.

8. The event-ordering certification method of claim 2, further comprising, for a plurality of event-ordering requests from the user apparatus:

a sequential aggregation tree storing step where the certification apparatus stores an information about the sequential aggregation tree produced at the event-ordering request aggregating step; and,

assuming that: the late complementary information of a leaf a1 determined at the point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as "late complementary

information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

5 a registration point storing step where the certification apparatus stores an information about the registration points of the plural event-ordering requests, wherein

10 at the certificate drafting step, the certification apparatus drafts a certificate for the new registration point from the information stored at both of the sequential aggregation tree storing step and the registration point storing step by integrating: the sequential assigned data-item of the new registration point; the first sequential aggregation tree specifying information for specifying the sequential aggregation tree and the leaf thereof both having the sequentially assigned data-item assigned thereto; the immediate complementary information of the new registration point; and the late complementary information of all of the passed  
15 registration points of the user apparatus at the new registration point.

9. The event-ordering certification method of claim 2, further comprising, for a plurality of event-ordering requests from the user apparatus:

20 a sequential aggregation tree storing step where the certification apparatus stores an information about the sequential aggregation tree produced at the event-ordering request aggregating step; and,

assuming that: the late complementary information of a leaf a1 determined at the point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as "late complementary  
25 information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

a registration point storing step where the certification apparatus stores an information about an immediately preceding registration point to the new  
30 registration point, wherein

at the certificate drafting step, the certification apparatus drafts a certificate for the new registration point from the information stored at both of the sequential aggregation tree storing step and the registration point storing step by integrating: the sequential assigned data-item of the new registration point; the sequential aggregation tree specifying information for specifying the sequential aggregation tree and the leaf thereof both having the sequentially assigned data-item assigned thereto; the immediate complementary information of the new registration point; and the late complementary information of the immediately preceding registration point of the user apparatus at the new registration point.

10

10. The event-ordering certification method of claim 8 or 9, wherein at the sequential aggregation tree storing step, the certification apparatus stores respective positions of nodes in the sequential aggregation tree, which have been subjected to an assignment, and respective assigned values for the nodes, as the information about the sequential aggregation tree.

15

11. The event-ordering certification method of claim 9, wherein the certification apparatus stores the immediate complementary information of the new registration point and the late complementary information of the immediately preceding registration point of the user apparatus at the new registration point, individually in stack.

20

12. The event-ordering certification method of any one of claims 8 to 11, further comprising an electronic information publishing step where the certification apparatus electronically publishes the root value of the sequential aggregation tree after completing the regular time interval.

25

13. The event-ordering certification method of any one of claims 8 to 12, further comprising a user's side electronic information publishing step where when the certification apparatus stops an operation thereof or vanishes data

30

necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval, the user apparatus electronically publishes both positional information and assigned values for one or more nodes whose assigned values are calculable and whose parents' assigned values are not calculable, from the certificates that the user apparatus has already received and stored by the time of stopping the operation of the certification apparatus or vanishing the data.

14. The event-ordering certification method of any one of claims 8 to 13, wherein at the event-ordering request aggregating step after completing the regular time interval, the certification apparatus assigns the root value of the sequential aggregation tree to a leaf of a next sequential aggregation tree so as to form the immediate complementary information about a new registration point assigned to the leaf of the next sequential aggregation tree.

15. An event-ordering certification audit method for an event-ordering certification system having at least one user apparatus performing an event-ordering request for certifying a chronological sequence of a certain event in time-series events generating a designated digital information, a certification apparatus for drafting a certificate for the event-ordering request of the user apparatus, an audit apparatus for auditing authenticity of the certificate and a communication network for connecting the user apparatus, the certification apparatus and the audit apparatus with each other, the method comprising:

an event-ordering request receiving step where the certification apparatus receives a first event-ordering request from the user apparatus;

a sequentially assigned data-item calculating step where the certification apparatus drafts a sequentially assigned data-item from a digital information included in the first event-ordering request in accordance with a predetermined procedure;

an event-ordering request aggregating step where, in sequential

aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a directed tree from left thereof, the certification apparatus calculates assigned values for calculable nodes and a root value to be assigned for a root of each  
 5 sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

10 a certificate drafting step where the certification apparatus drafts a first certificate containing the sequentially assigned data-item and a first sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto;

15 a certificate sending step where the certification apparatus sends the first certificate to the user apparatus;

assuming that: a leaf of the sequential aggregation tree to which the first event-ordering request is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree  
 20 from the registration point is defined as a complementary information of the first certificate; and in the complementary information, a complementary information acquirable at a point of assigning the first event-ordering request to the sequential aggregation tree is defined as an immediate complementary information,

an audit certificate drafting step where the certification apparatus assigns a  
 25 plurality of audit requests to the sequential aggregation tree thereby drafting a plurality of audit certificates in the same way as drafting the certificate, acquires immediate complementary information for audit at the point of assigning the respective audit requests to the sequential aggregation tree, from the sequential aggregation tree and incorporates the immediate complementary information for  
 30 audit into the respective audit certificates;

an audit certificate sending step where the certification apparatus sends the audit certificates to the audit apparatus;

5 a complementary information request receiving step where after sending the first certificate to the user apparatus, the certification apparatus receives a request of the complementary information of the first certificate from the user apparatus;

10 a late complementary information drafting step where the certification apparatus acquires a second sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the request of the complementary information assigned thereto and a complementary information acquirable at the point of assigning the request of the complementary information, from the sequential aggregation tree, thereby forming a late complementary information;

15 a late complementary information sending step where the certification apparatus sends the late complementary information about the first certificate to the user apparatus;

an audit certificate receiving step where the audit apparatus receives the audit certificates from the certification apparatus;

20 an audit request receiving step where the audit apparatus receives an audit request for the first certificate from the user apparatus, the audit request containing the first certificate and the late complementary information about the first certificate;

25 a first audit certificate selecting step where the audit apparatus selects an audit certificate from the audit certificates on a basis of the first and second sequential aggregation tree specifying information in the audit request for the first certificate, the one audit certificate being generated after the first certificate and before the late complementary information in chronological sequence;

30 a first certificate audit step where the audit apparatus audits validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit certificate



selected at the first audit certificate selecting step coincides with an assigned value for the specified node calculated from the audit request for the first certificate or not and, where the audit apparatus further certifies a temporal context between a receipt time of the event-ordering request for the first certificate and a receipt time of the audit request for the audit certificate selected at the first audit certificate selecting step; and

an audit result sending step where the audit apparatus sends an audit result of the first certificate to the user apparatus.

10 16. The event-ordering certification audit method of claim 15, wherein:

the audit certificate receiving step further includes a step of acquiring a first time when the audit apparatus received the audit certificate selected at the first audit certificate selecting step, from a time offering apparatus; and

15 at the first certificate audit step, the audit apparatus incorporates a block-time certificate representing that the receipt time of the event-ordering request for the first certificate is temporally ahead of the first time into the audit result.

17. The event-ordering certification audit method of claim 15 or 16, further comprising

20 an audit late complementary information drafting step where after completing the regular time interval, the certification apparatus acquires all of the complementary information about the audit certificates drafted at the audit certificate drafting step, from the sequential aggregation tree thereby forming a late complementary information about the audit certificates;

25 an audit late complementary information sending step where the certification apparatus sends the late complementary information about the audit certificates to the audit apparatus;

30 a second audit certificate selecting step where the audit apparatus selects an audit certificate from the audit certificates on a basis of the first sequential

aggregation tree specifying information in the audit request for the first certificate, the audit certificate being generated before the first certificate in chronological sequence; and

5 a second certificate audit step where the audit apparatus audits validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit request for the first certificate coincides with an assigned value for the specified node calculated from the audit certificate selected at the second audit certificate selecting step and the late complementary information in the audit certificate or  
10 not and, where the audit apparatus further certifies a temporal context' between a receipt time of the event-ordering request for the first certificate and a receipt time of the audit request for the audit certificate selected at the second audit certificate selecting step.

15 18. The event-ordering certification audit method of claim 17, further comprising, for a second event-ordering request from the user apparatus or the other user apparatus, an inter-certificate ordering judgment step where the audit apparatus judges the temporal context between the receipt time of the event-ordering request for the first certificate and the receipt time of the  
20 event-ordering request for the second certificate on a basis of validation of the audit result for the second certificate drafted for the second event-ordering request and the first sequential aggregation tree specifying information about the first and second certificates, wherein

at the audit result sending step, the audit apparatus incorporates a  
25 chronological sequence in receiving the requests in between the plural certificates into the audit result.

19. The event-ordering certification audit method of claim 17 or 18, further comprising:

30 a root-value calculating step where the audit apparatus calculates a root

value of the sequential aggregation tree from the plural audit certificates and the late complementary information about the plural audit certificates; and

5 a root-value validation step where the audit apparatus verifies whether a root value of the sequential aggregation tree published electronically coincides with the root value calculated at the root-value calculating step.

20. The event-ordering certification audit method of any one of claims 17 to 19, further comprising an audit complementary information sending step where the audit apparatus sends the audit certificate selected at the first audit certificate selecting step and the late complementary information about the audit certificate to  
10 the user apparatus.

21. The event-ordering certification audit method of any one of claims 17 to 20, wherein:

15 the audit certificate receiving step further includes a step of acquiring a second time when the audit apparatus sent the audit certificate selected at the second audit certificate selecting step to the user apparatus, from a time offering apparatus; and

20 at the second certificate audit step, the audit apparatus incorporates a block-time certificate representing that the receipt time of the event-ordering request for the first certificate is temporally ahead of the second time into the audit result.

22. The event-ordering certification audit method of any one of claims 15 to 25 21, wherein at the first certificate audit step, the audit apparatus applies a digital signature on the audit result.

23. An event-ordering certification apparatus connected to both a user apparatus performing an event-ordering request for certifying a chronological  
30 sequence of a certain event in time-series events generating a designated digital

information thereby promoting the event-ordering certification apparatus to draft a certificate and an audit apparatus for auditing authenticity of the certificate through a communication network mutually, for drafting the certificate, for the event-ordering request of the user apparatus, the event-ordering certification apparatus comprising:

event-ordering request receiving means configured to receive the event-ordering request from the user apparatus;

sequentially assigned data-item calculating means configured to draft a sequentially assigned data-item from a digital information included in the event-ordering request in accordance with a predetermined procedure;

event-ordering request aggregating means configured, in sequential aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a directed tree from left thereof, to calculate assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

certificate drafting means configured to draft a certificate containing the sequentially assigned data-item and a first sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto;

certificate sending means configured to send the certificate to the user apparatus;

assuming that: a leaf of the sequential aggregation tree to which the event-ordering request is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the

certificate; and in the complementary information, a complementary information acquirable at a point of assigning the event-ordering request to the sequential aggregation tree is defined as an immediate complementary information,

audit certificate drafting means configured, after assigning the  
5 event-ordering request to the sequential aggregation tree, to assign a first audit request to the sequential aggregation tree thereby drafting a first audit certificate in the same way as drafting the certificate, acquire a first immediate complementary information for audit at the point of assigning the first audit request to the sequential aggregation tree, from the sequential aggregation tree and incorporate  
10 the first immediate complementary information into the first audit certificate;

audit certificate sending means configured to send the first audit certificate to the audit apparatus;

complementary information request receiving means configured, after assigning the first audit request to the sequential aggregation tree, to receive a  
15 request of the complementary information of the certificate from the user apparatus;

late complementary information drafting means configured to acquire a second sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the request of the  
20 complementary information assigned thereto and a complementary information acquirable at the point of assigning the request of the complementary information, from the sequential aggregation tree, thereby forming a late complementary information; and

complementary information sending means configured to send the late  
25 complementary information about the certificate to the user apparatus.

24. The event-ordering certification apparatus of claim 23, wherein the certificate drafting means incorporates the immediate complementary information of the certificate into the first sequential aggregation tree specifying information.

25. The event-ordering certification apparatus of claim 23 or 24, wherein:

the audit certificate drafting means further includes means configured, before assigning the event-ordering request to the sequential aggregation tree, to assign a second audit request to the sequential aggregation tree thereby drafting a  
5 second audit certificate in the same way as drafting the certificate, acquire a second immediate complementary information for audit at the point of assigning the second audit request to the sequential aggregation tree from the sequential aggregation tree and incorporate the second immediate complementary information into the second audit certificate; the event-ordering certification  
10 apparatus further comprises:

an audit late complementary information drafting means configured, after completing the regular time interval, to acquire all of the complementary information about the first and second audit certificates drafted at the audit certificate drafting step, from the sequential aggregation tree thereby forming a late  
15 complementary information about the first and second audit certificates; and

an audit late complementary information sending means configured to send the late complementary information about the first and second audit certificates to the audit apparatus.

26. The event-ordering certification apparatus of any one of claims 23 to 25, wherein the sequentially assigned data-item calculating means calculates a result value obtained by applying a designated collision-resistant hash function on the digital information contained in the event-ordering request, as the sequentially  
20 assigned data-item.

27. The event-ordering certification apparatus of any one of claims 23 to 26, wherein the certificate drafting means applies a digital signature on the certificate  
25 drafted.

28. The event-ordering certification apparatus of any one of claims 23 to 27,  
30

further comprising electronic information publishing means configured to publish the root value of the sequential aggregation tree electronically after completing the regular time interval.

5 29. The event-ordering certification apparatus of any one of claims 23 to 28, wherein for a plurality of event-ordering requests from the user apparatus, the certificate sending means further includes means configured to send respective certificates for the event-ordering requests in chronological sequence of assigning the event-ordering requests to the sequential aggregation tree.

10

30. The event-ordering certification apparatus of claim 24, further comprising, for a plurality of event-ordering requests from the user apparatus:

sequential aggregation tree storing means configured to store an information about the sequential aggregation tree produced at the event-ordering request aggregating step; and,

15

assuming that: the late complementary information of a leaf a1 determined at the point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as "late complementary information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

20

registration point storing means configured to store an information about the registration points of the plural event-ordering requests, wherein

the certificate drafting means integrates, from the information stored by both of the sequential aggregation tree storing means and the registration point storing means, the sequential assigned data-item of the new registration point, the first sequential aggregation tree specifying information for specifying the sequential aggregation tree and the leaf thereof both having the sequentially assigned data-item assigned thereto, the immediate complementary information of the new registration point and the late complementary information of all of the

30

passed registration points of the user apparatus at the new registration point, thereby drafting a certificate for the new registration point.

31. The event-ordering certification apparatus of claim 24, further comprising,  
5 for a plurality of event-ordering requests from the user apparatus,

sequential aggregation tree storing step means configured to store an information about the sequential aggregation tree produced at the event-ordering request aggregating means; and,

assuming that: the late complementary information of a leaf a1  
10 determined at the point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as "late complementary information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

15 registration point storing means configured to store an information about an immediately preceding registration point to the new registration point, wherein

the certificate drafting means integrates, from the information stored by both of the sequential aggregation tree storing means and the registration point storing means, the sequential assigned data-item of the new registration point, the  
20 sequential aggregation tree specifying information for specifying the sequential aggregation tree and the leaf thereof both having the sequentially assigned data-item assigned thereto, the immediate complementary information of the new registration point and the late complementary information of the immediately preceding registration point of the user apparatus at the new registration point,  
25 thereby drafting a certificate for the new registration point.

32. The event-ordering certification apparatus of claim 30 or 31, wherein the sequential aggregation tree storing means stores respective positions of nodes in the sequential aggregation tree, which have been subjected to an assignation, and  
30 respective assigned values for the nodes, as the information about the sequential



aggregation tree.

33. The event-ordering certification apparatus of claim 31, wherein the sequential aggregation tree storing means includes a first stack to store the  
5 immediate complementary information of the new registration point and a second stack to store the late complementary information of the immediately preceding registration point of the user apparatus at the new registration point.

34. The event-ordering certification apparatus of any one of claims 30 to 33,  
10 further comprising electronic information publishing means configured to electronically publish the root value of the sequential aggregation tree after completing the regular time interval.

35. The event-ordering certification apparatus of any one of claims 30 to 34,  
15 wherein when the event-ordering certification apparatus stops an operation thereof or vanishes data necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval, the user apparatus further includes user's side electronic information publishing means configured to electronically publish both positional information and assigned values for one or  
20 more nodes whose assigned values are calculable and whose parents' assigned values are not calculable, from the certificates that the user apparatus has already received and stored by the time of stopping the operation of the certification apparatus or vanishing the data.

25 36. The event-ordering certification apparatus of any one of claims 30 to 35, wherein after completing the regular time interval, the event-ordering request aggregating means assigns the root value of the sequential aggregation tree to a leaf of a next sequential aggregation tree so as to form the immediate complementary information about a new registration point assigned to the leaf of  
30 the next sequential aggregation tree.

37. An event-ordering certification audit apparatus connected to both at least one user apparatus performing an event-ordering request for certifying a chronological sequence of a certain event in time-series events generating a designated digital information and a certification apparatus for drafting a certificate for the event-ordering request of the user apparatus, through a communication network, for auditing authenticity of the certificate, wherein the certification apparatus comprises:

event-ordering request receiving means configured to receive a first event-ordering request from the user apparatus;

sequentially assigned data-item calculating means configured to draft a sequentially assigned data-item from a digital information included in the first event-ordering request in accordance with a predetermined procedure;

event-ordering request aggregating means configured, in sequential aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a directed tree from left thereof, to calculate assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

certificate drafting means configured to draft a first certificate containing the sequentially assigned data-item and a first sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto;

certificate sending means configured to send the first certificate to the user apparatus;

assuming that: a leaf of the sequential aggregation tree to which the first

event-ordering request is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the first certificate; and in the complementary information, a complementary information  
5     acquirable at a point of assigning the first event-ordering request to the sequential aggregation tree is defined as an immediate complementary information,

audit certificate drafting means configured to assign a plurality of audit requests to the sequential aggregation tree thereby drafting a plurality of audit certificates in the same way as drafting the certificate, acquire immediate  
10     complementary information for audit at the point of assigning the respective audit requests to the sequential aggregation tree from the sequential aggregation tree and incorporate the immediate complementary information for audit into the respective audit certificates;

audit certificate sending means configured to send the audit certificates to  
15     the audit apparatus;

complementary information request receiving means configured, after sending the first certificate to the user apparatus, to receive a request of the complementary information of the first certificate from the user apparatus;

late complementary information drafting means configured to acquire a  
20     second sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the request of the complementary information assigned thereto and a complementary information acquirable at the point of assigning the request of the complementary information, from the sequential aggregation tree, thereby forming a late complementary  
25     information; and

late complementary information sending means configured to send the late complementary information about the first certificate to the user apparatus, and

wherein the event-ordering certification audit apparatus comprises:

30     audit certificate receiving means configured to receive the audit

certificates from the certification apparatus;

audit request receiving means configured to receive an audit request for the first certificate from the user apparatus, the audit request containing the first certificate and the late complementary information about the first certificate;

5 first audit certificate selecting means configured to select an audit certificate from the audit certificates on a basis of the first and second sequential aggregation tree specifying information in the audit request for the first certificate, the audit certificate being generated after the first certificate and before the late complementary information in chronological sequence;

10 first certificate audit means configured to audit validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit certificate selected by the first audit certificate selecting means coincides with an assigned value for the specified node calculated from the audit request for the first  
15 certificate or not and, also configured to further certify a temporal context between a receipt time of the event-ordering request for the first certificate and a receipt time of the audit request for the audit certificate selected by the first audit certificate selecting means; and

audit result sending means configured to send an audit result of the first  
20 certificate to the user apparatus.

38. The event-ordering certification audit apparatus of claim 37, wherein:

the audit certificate receiving means further includes means configured to acquire a first time when the audit apparatus received the audit certificate selected  
25 by the first audit certificate selecting means, from a time offering apparatus; and

the first certificate audit means incorporates a block-time certificate representing that the receipt time of the event-ordering request for the first certificate is temporally ahead of the first time into the audit result.

30 39. The event-ordering certification audit apparatus of claim 37 or 38, wherein

the certification apparatus further comprises:

audit late complementary information drafting means configured to acquire all of the complementary information about the audit certificates drafted by the audit certificate drafting means from the sequential aggregation tree after  
5 completing the regular time interval, thereby forming a late complementary information about the audit certificates; and

audit late complementary information sending means configured to send the late complementary information about the audit certificates to the audit apparatus, and

10 wherein the event-ordering certification audit apparatus further comprises:

second audit certificate selecting means configured to select an audit certificate from the audit certificates on a basis of the first sequential aggregation tree specifying information in the audit request for the first certificate, the audit certificate being generated before the first certificate in chronological sequence;  
15 and

second certificate audit means configured to audit validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit request for the first certificate coincides with an assigned value for the specified node calculated from the audit certificate selected by the second audit certificate  
20 selecting means and the late complementary information in the audit certificate or not and, where the audit apparatus further certifies a temporal context between a receipt time of the event-ordering request for the first certificate and a receipt time of the audit request for the audit certificate selected by the second audit certificate  
25 selecting means.

40. The event-ordering certification audit apparatus of claim 39, further comprising, for a second event-ordering request from the user apparatus or the other user apparatus, inter-certificate ordering judgment means configured to judge  
30 the temporal context between the receipt time of the event-ordering request for the

first certificate and the receipt time of the event-ordering request for the second certificate on a basis of validation of the audit result for the second certificate drafted for the second event-ordering request and the first sequential aggregation tree specifying information about the first and second certificates, wherein

5       the audit result sending means incorporates a chronological sequence in receiving the requests in between the plural certificates into the audit result.

41.     The event-ordering certification audit apparatus of claim 39 or 40, further comprising:

10       root-value calculating means configured to calculate a root value of the sequential aggregation tree from the plural audit certificates and the late complementary information about the plural audit certificates; and

       root-value validation means configured to verify whether a root value of the sequential aggregation tree published electronically coincides with the root  
15     value calculated at the root-value calculating step.

42.     The event-ordering certification audit apparatus of any one of claims 39 to 41, further comprising audit complementary information sending means configured to send the audit certificate selected by the first audit certificate  
20     selecting means and the late complementary information about the audit certificate to the user apparatus.

43.     The event-ordering certification audit apparatus of any one of claims 39 to 42, wherein:

25       the audit certificate receiving means further includes means configured to acquire a second time when the event-ordering certification audit apparatus sent the audit certificate selected by the second audit certificate selecting means to the user apparatus, from a time offering apparatus; and

       the second certificate audit means incorporates a block-time certificate  
30     representing that the receipt time of the event-ordering request for the first

certificate is temporally ahead of the second time into the audit result.

44. The event-ordering certification audit apparatus of any one of claims 39 to 42, wherein the first certificate audit means applies a digital signature on the audit  
5 result.

45. An event-ordering certification program for allowing the certification apparatus to perform the respective steps of the event-ordering certification method of any one of claims 1 to 14.

46. An event-ordering certification audit program for allowing the certification apparatus to perform the respective steps of the event-ordering certification audit method of any one of claims 15 to 22.

47. A program for validation of event-ordering certificates for a user apparatus in an event-ordering certification audit system where at least one user apparatus performing an event-ordering request for certifying a chronological sequence of a certain event in time-series events generating a designated digital information, a certification apparatus for drafting a certificate for the event-ordering request of the user apparatus and an audit apparatus for auditing authenticity of the certificate are  
15 20 connected with each other through a communication network,

wherein the certification apparatus comprises:

event-ordering request receiving means configured to receive a first event-ordering request from the user apparatus;

25 sequentially assigned data-item calculating means configured to draft a sequentially assigned data-item from a digital information included in the first event-ordering request in accordance with a predetermined procedure;

event-ordering request aggregating means configured, in sequential aggregation trees each of which is completed at regular time intervals by  
30 sequentially assigning a series of sequentially assigned data-items to leaves of a

directed tree from left thereof, to calculate assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by  
 5 applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

certificate drafting means configured to draft a first certificate containing the sequentially assigned data-item and a first sequential aggregation tree  
 10 specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto;

certificate sending means configured to send the first certificate to the user apparatus;

assuming that: a leaf of the sequential aggregation tree to which the first  
 15 event-ordering request is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the first certificate; and in the complementary information, a complementary information acquirable at a point of assigning the first event-ordering request to the sequential  
 20 aggregation tree is defined as an immediate complementary information,

audit certificate drafting means configured to assign a plurality of audit requests to the sequential aggregation tree thereby drafting a plurality of audit certificates in the same way as drafting the certificate, acquire immediate complementary information for audit at the point of assigning the respective audit  
 25 requests to the sequential aggregation tree from the sequential aggregation tree and incorporate the immediate complementary information for audit into the respective audit certificates;

audit certificate sending means configured to send the audit certificates to the audit apparatus;

30 complementary information request receiving means configured, after



sending the first certificate to the user apparatus, to receive a request of the complementary information of the first certificate from the user apparatus;

late complementary information drafting means configured to acquire a second sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the request of the complementary information assigned thereto and a complementary information acquirable at the point of assigning the request of the complementary information, from the sequential aggregation tree, thereby forming a late complementary information; and

late complementary information sending means configured to send the late complementary information about the first certificate to the user apparatus, and

wherein the audit apparatus comprises:

audit certificate receiving means configured to receive the audit certificates from the certification apparatus;

audit request receiving means configured to receive an audit request for the first certificate from the user apparatus, the audit request containing the first certificate and the late complementary information about the first certificate;

first audit certificate selecting means configured to select an audit certificate from the audit certificates on a basis of the first and second sequential aggregation tree specifying information in the audit request for the first certificate, the audit certificate being generated after the first certificate and before the late complementary information in chronological sequence;

first certificate audit means configured to audit validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit certificate selected by the first audit certificate selecting means coincides with an assigned value for the specified node calculated from the audit request for the first certificate or not and, also configured to further certify a temporal context between a receipt time of the event-ordering request for the first certificate and a receipt

time of the audit request for the audit certificate selected by the first audit certificate selecting means; and

audit result sending means configured to send an audit result of the first certificate to the user apparatus, and

5 wherein the event-ordering certification program allows the user apparatus to perform:

an event-ordering request sending step of sending the first event-ordering request to the certification apparatus;

10 a certificate receiving step of receiving first event-ordering request from the certification apparatus

a complementary information request sending step of sending the request of the complementary information of the first certificate to the certification apparatus;

15 a complementary information receiving step of receiving the complementary information of the first certificate from the certification apparatus;

an audit request sending step of sending the audit request to the audit apparatus; and

an audit result receiving step of receiving the audit result for the first certificate.

20

48. The program for validation of event-ordering certificates of claim 47, wherein:

25 the audit certificate receiving means further includes means configured to acquire a first time when the audit apparatus received the audit certificate selected by the second audit certificate-selecting means from a time offering apparatus; and

the first certificate audit means incorporates a block-time certificate representing that the receipt time of the event-ordering request for the first certificate is temporally ahead of the first time into the audit result, and

30 wherein the program for validation of event-ordering certificates allows the user apparatus to perform an event-ordering request drafting step of acquiring a

third time at the point of sending the first event-ordering request to the certification apparatus from the time offering apparatus and incorporating a value as a result of calculating the third time in accordance with a designated procedure into the first event-ordering request.

5

49. The program for validation of event-ordering certificates of claim 47 or 48, wherein the certification apparatus further comprises:

audit late complementary information drafting means configured to acquire all of the complementary information about the audit certificates drafted by the audit certificate drafting means from the sequential aggregation tree after completing the regular time interval, thereby forming a late complementary information about the audit certificates; and

audit late complementary information sending means configured to send the late complementary information about the audit certificates to the audit apparatus, and

15

wherein the audit apparatus further comprises:

second audit certificate selecting means configured to select an audit certificate from the audit certificates on a basis of the first sequential aggregation tree specifying information in the audit request for the first certificate, the audit certificate being generated before the first certificate in chronological sequence; and

20

second certificate audit means configured to audit validity of the first certificate by verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the audit request for the first certificate coincides with an assigned value for the specified node calculated from the audit certificate selected by the second audit certificate selecting means and the late complementary information in the audit certificate or not and, where the audit apparatus further certifies a temporal context between a receipt time of the event-ordering request for the first certificate and a receipt time of the audit request for the audit certificate selected by the second audit certificate

30

selecting means.

50. The program for validation of event-ordering certificates of claim 49, wherein:

5 the audit apparatus includes, for a second event-ordering request from the user apparatus or the other user apparatus, inter-certificate ordering judgment means configured to judge the temporal context between the receipt time of the event-ordering request for the first certificate and the receipt time of the event-ordering request for the second certificate on a basis of validation of the  
10 audit result for the second certificate drafted for the second event-ordering request and the first sequential aggregation tree specifying information about the first and second certificates;

the audit result sending means incorporates a chronological sequence in receiving the requests in between the first and second certificates into the audit  
15 result; and

the audit request for the first certificate includes a request for judging its chronological sequence in relation to the second certificate.

51. The program for validation of event-ordering certificates of claim 49, wherein:

20 the audit apparatus includes audit complementary information sending means configured to send the audit certificate selected by the first audit certificate selecting means and the late complementary information about the audit certificate to the user apparatus; and

25 the program for validation of event-ordering certificates allows the user apparatus to perform a step of receiving the audit certificate and its late complementary information sent from the audit apparatus.

52. The program for validation of event-ordering certificates of any one of  
30 claims 48 to 51, wherein:

the audit certificate receiving means further includes means configured to acquire a second time when the event-ordering certification audit apparatus sent the audit certificate selected by the second audit certificate selecting means to the user apparatus, from a time offering apparatus;

5       the second certificate audit means incorporates a block-time certificate representing that the receipt time of the event-ordering request for the first certificate is temporally ahead of the second time into the audit result; and

10       the program for validation of event-ordering certificates allows the user apparatus to perform an event-ordering request drafting step of acquiring a third time at the point of sending the first event-ordering request to the certification apparatus from the time offering apparatus and incorporating a value as a result of calculating the third time in accordance with a designated procedure into the first event-ordering request.

15   53.   The program for validation of event-ordering certificates of any one of claims 47 to 52, wherein the program for validation of event-ordering certificates allows the user apparatus to perform:

20       a root-value calculating step of calculating a root value of the sequential aggregation tree from the first certificate sent from the certification apparatus and all of the late complementary information about the first certificate acquired after completing the regular time interval; and

25       a root-value validation step of verifying whether a root value for the sequential aggregation tree published electronically after completing the regular time interval coincides with the root value calculated at the root-value calculating step.

30   54.   A program for validation of event-ordering certificates for allowing a computer to verify authenticity of certificates, the computer being connected to first and second user apparatuses, each of which performs an event-ordering request for certifying a chronological sequence of a certain event in time-series

events generating a designated digital information, and an event-ordering certification apparatus for drafting the certificates for a plurality of event-ordering requests of the first and second user apparatuses through a communication network,

5           wherein the event-ordering certification apparatus comprises:

          event-ordering request receiving means configured to receive the event-ordering requests from the first and second user apparatuses;

          sequentially assigned data-item calculating means configured to draft sequentially assigned data-items from digital information included in the  
10       event-ordering requests in accordance with a predetermined procedure;

          event-ordering request aggregating means configured, in sequential aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a directed tree from left thereof, to calculate assigned values for calculable nodes  
15       and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent  
20       in common are connected;

          sequential aggregation tree storing means configured to store an information about the sequential aggregation trees produced by the event-ordering request aggregating means;

          assuming that: a leaf of the sequential aggregation tree to which the  
25       sequentially-assigned data-item drafted from each of the event-ordering requests is assigned is defined as a registration point; an information about nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the registration point; in the complementary information, a complementary information acquirable at a point of  
30       assigning each of the sequentially assigned data-item to the sequential aggregation

tree is defined as an immediate complementary information, while a complementary information acquirable after the point of assigning each of the sequentially assigned data-item to the sequential aggregation tree is defined as a late complementary information; the late complementary information of a leaf a1  
 5 determined at a point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as "late complementary information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

10 registration point storing means configured to store an information about the registration points of the event-ordering requests with respect to each of the user apparatuses;

certificate drafting means configured to integrate, from the information stored in the respective storing means, a sequentially assigned data-item for the  
 15 new registration point, a sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto, an immediate complementary information about the new registration point and a late complementary information of all past registration points of each of the user apparatuses, thereby  
 20 drafting a certificate for the new registration point; and

certificate sending means configured to send the certificates to the user apparatuses;

wherein each of the user apparatuses comprises:

event-ordering request sending means configured to send the  
 25 event-ordering requests to the event-ordering certification apparatus;

certificate receiving means configured to receive the certificates for the event-ordering requests from the event-ordering certification apparatus;

certificate storing means configured to store the certificates received;

validation request sending means configured to send a certificate for  
 30 validation to the computer; and

validation result receiving means configured to receive a validation result of the certificate for validation from the computer;

wherein the program for validation of event-ordering certificates allows the computer to perform:

5        a certificate receiving step of receiving two certificates for validation from the first and second user apparatuses respectively or two certificates for validation from the first user apparatus;

10       assuming that one of the two certificates judged as being temporally former in publishing order is a first certificate, while the other of the two certificates judged as being temporally latter in publishing order is a second certificate, based on the sequential aggregation tree specifying information of the two certificates received,

15       a sequential aggregation tree specifying information sending step of sending the sequential aggregation tree specifying information in the second certificate to the user apparatus receiving the first certificate;

      a late complementary information receiving step of receiving the late complementary information about the first certificate at a registration point after publishing the second certificate, from the user apparatus receiving the first certificate;

20       a validation step of verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the second certificate coincides with an assigned value for the specified node calculated from the first certificate and the late complementary information or not, thereby certifying validity of the first and second certificates and that the  
25       registration point of the first certificate is temporally ahead of the registration point of the second certificate, based on a validation result; and

      a validation result sending step of sending the validation result to both or either of the first and second user apparatuses.

30    55.    The program for validation of event-ordering certificates of claim 54,



wherein when the event-ordering certification apparatus stops an operation thereof or vanishes data necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval,

5 each of the user apparatuses includes user's side electronic information publishing means configured to electronically publish both positional information and assigned values for one or more nodes whose assigned values are calculable and whose parents' assigned values are not calculable, from the certificates that the user apparatus has already received and stored by the time of stopping the operation of the certification apparatus or vanishing the data, and

10 when the event-ordering certification apparatus stops an operation thereof or vanishes data necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval, the program for validation of event-ordering certificates allows the computer to perform a "by user's side publishing value" validation step of verifying that both received data at  
15 the certificate receiving step and received data at the late complementary information receiving step are not tampered by judging whether each assigned value for the one or more nodes published by the user apparatus through the user's side electronic information publishing means coincides with an assigned value calculated by both the received data at the certificate receiving step and the  
20 received data at the late complementary information receiving step.

56. A program for validation of event-ordering certificates for allowing a computer to verify authenticity of certificates, the computer being connected to first and second user apparatuses, each of which performs an event-ordering  
25 request for certifying a chronological sequence of a certain event in time-series events generating a designated digital information, and an event-ordering certification apparatus for drafting the certificates for a plurality of event-ordering requests of the first and second user apparatuses through a communication network,

30 wherein the event-ordering certification apparatus comprises:

event-ordering request receiving means configured to receive the event-ordering requests from the first and second user apparatuses;

sequentially assigned data-item calculating means configured to draft sequentially assigned data-items from digital information included in the event-ordering requests in accordance with a predetermined procedure;

event-ordering request aggregating means configured, in sequential aggregation trees each of which is completed at regular time intervals by sequentially assigning a series of sequentially assigned data-items to leaves of a directed tree from left thereof, to calculate assigned values for calculable nodes and a root value to be assigned for a root of each sequential aggregation tree after completion of each regular time interval, in accordance with a calculating method of establishing, as an assigned value for a parent, a result value obtained by applying a designated collision-resistant hash function on a juncture value to which respective assigned values assigned to a plurality of nodes having a parent in common are connected;

sequential aggregation tree storing means configured to store an information about the sequential aggregation trees produced by the event-ordering request aggregating means;

assuming that: a leaf of the sequential aggregation tree to which the sequentially-assigned data-item drafted from each of the event-ordering requests is assigned is defined as a registration point; an information about other nodes necessary to calculate a root value of the sequential aggregation tree from the registration point is defined as a complementary information of the registration point; in the complementary information, a complementary information acquirable at a point of assigning each of the sequentially assigned data-item to the sequential aggregation tree is defined as an immediate complementary information, while a complementary information acquirable after the point of assigning each of the sequentially assigned data-item to the sequential aggregation tree is defined as a late complementary information; the late complementary information of a leaf a1 determined at a point of completing an assignation for a leaf a2 on the right of the

leaf a1 in the sequential aggregation tree is defined as "late complementary information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

5 registration point storing means configured to store an information about an immediately preceding registration point with respect to each of the user apparatuses;

certificate drafting means configured to integrate, from the information stored in the respective storing means, a sequentially assigned data-item for the new registration point, a sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the sequentially assigned data-item assigned thereto, an immediate complementary information about the new registration point and a late complementary information about the immediately preceding registration point of each of the user apparatuses at the new registration point, thereby drafting a certificate for the new registration point; and

15 certificate sending means configured to send the certificates to the user apparatuses;

defining that a rightmost registration point of the respective registration points of each of the user apparatuses is referred to as a provisional terminal point and that to calculate all of the complementary information about a designated registration point acquirable at a point of completing an assignment for the provisional terminal point is referred to as an incremental completion for a certificate of the designated registration point,

25 wherein each of the user apparatuses comprises:

event-ordering request sending means configured to send the event-ordering requests to the event-ordering certification apparatus;

certificate receiving means configured to receive the certificates for the event-ordering requests from the event-ordering certification apparatus;

30 certificate storing means configured to store the certificates received;

incremental completion means configured to perform the incremental completion to a certificate for validation of the plural certificates received and stored;

validation request sending means configured to send a certificate for validation to the computer; and

validation result receiving means configured to receive a validation result of the certificate for validation from the computer;

wherein the program for validation of event-ordering certificates allows the computer to perform:

10 a certificate receiving step of receiving two certificates for validation from the first and second user apparatuses respectively or two certificates for validation from the first user apparatus;

assuming that one of the two certificates judged as being temporally former in publishing order is a first certificate, while the other of the two  
15 certificates judged as being temporally latter in publishing order is a second certificate, based on the sequential aggregation tree specifying information of the two certificates received,

a sequential aggregation tree specifying information sending step of sending the sequential aggregation tree specifying information in the second  
20 certificate to the user apparatus receiving the first certificate;

a late complementary information receiving step of receiving the late complementary information about the first certificate at a registration point after publishing the second certificate, from the user apparatus receiving the first certificate;

25 a validation step of verifying, for a specified node in the sequential aggregation tree, whether an assigned value for the specified node contained in the second certificate coincides with an assigned value for the specified node calculated from the first certificate and the late complementary information or not, thereby certifying validity of the first and second certificates and that the  
30 registration point of the first certificate is temporally ahead of the registration point

of the second certificate, based on a validation result; and

a validation result sending step of sending the validation result to both or either of the first and second user apparatuses.

5 57. The program for validation of event-ordering certificates of claim 56, wherein when the event-ordering certification apparatus stops an operation thereof or vanishes data necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval,

10 each of the user apparatuses includes user's side electronic information publishing means configured to electronically publish both positional information and assigned values for one or more nodes whose assigned values are calculable and whose parents' assigned values are not calculable, from the certificates that the user apparatus has already received and stored by the time of stopping the operation of the certification apparatus or vanishing the data, and

15 when the event-ordering certification apparatus stops an operation thereof or vanishes data necessary for calculating the root value of the sequential aggregation tree before completing the regular time interval, the program for validation of event-ordering certificates allows the computer to perform a "by user's side publishing value" validation step of verifying that both received data at  
20 the certificate receiving step and received data at the late complementary information receiving step are not tampered by judging whether each assigned value for the one or more nodes published by the user apparatus through the user's side electronic information publishing means coincides with an assigned value calculated by both the received data at the certificate receiving step and the  
25 received data at the late complementary information receiving step.

58. The program for validation of event-ordering certificates of claim 47, wherein the certification apparatus further comprising, for a plurality of event-ordering requests from the user apparatus:

30 sequential aggregation tree storing means configured to store an

information about the sequential aggregation tree produced by the event-ordering request aggregating means;

assuming that: the late complementary information of a leaf a1 determined at the point of completing an assignation for a leaf a2 on the right of the leaf a1 in the sequential aggregation tree is defined as "late complementary  
5 information of the leaf a1 at the leaf a2"; and further a leaf of the sequential aggregation tree to which the sequential assigned data-item drafted by a new event-ordering request is defined as a new registration point,

registration point storing means configured to store an information about  
10 the immediately preceding registration point,

certificate drafting means configured to integrate, from the information stored in the respective storing means, a sequentially assigned data-item for the new registration point, a sequential aggregation tree specifying information for specifying the sequential aggregation tree and a leaf thereof both having the  
15 sequentially assigned data-item assigned thereto, an immediate complementary information about the new registration point and a late complementary information about the immediately preceding registration point of each of the user apparatuses at the new registration point, thereby drafting a certificate for the new registration point; and

20 certificate sending means configured to send the certificates to the user apparatuses; and

defining that a rightmost registration point of the respective registration points of each of the user apparatuses is referred to as a provisional terminal point and that to calculate all of the complementary information about a designated  
25 registration point acquirable at a point of completing an assignment for the provisional terminal point is referred to as an incremental completion for a certificate of the designated registration point, wherein the program for validation of event-ordering certificates allows the computer to perform:

an event-ordering request sending step of sending the event-ordering  
30 requests to the certification apparatus;

a certificate receiving step of receiving the certificates for the event-ordering requests from the certification apparatus;

a certificate storing step of storing the certificates received; and

an incremental completion step of performing the incremental completion  
5 to a certificate for validation of the plural certificates received and stored.

59. The program for validation of event-ordering certificates of any one of claims 56 to 58, wherein the incremental completion is carried out with the use of the certificates that the user apparatus received from the certification apparatus and  
10 further stored therein and without forming a tree structure.

60. The program for validation of event-ordering certificates of claim 59, wherein for respective elements forming the complementary information about a designated registration point acquirable at a point of completing an assignment for  
15 the provisional terminal point, the incremental completion is carried out by firstly selecting one certificate out of one or more certificates that the user apparatus received from the certification apparatus and further stored therein, the one certificate containing either the elements directly or information enough to calculate the elements, and secondly calculating the elements from the one  
20 certificate selected.

61. The program for validation of event-ordering certificates of claim 59, wherein the complementary information is carried out to all of registration points positioned on the left of the provisional terminal point of the user apparatus.  
25

62. The program for validation of event-ordering certificates of claim 61, defining that, for one registration point a1 of the user apparatus on the left of the provisional terminal point and another registration point a2 of the user apparatus closest to the point a1 on a left side thereof, to calculate all of the complementary  
30 information about the registration point a2 acquirable at a point of completing an

assignment of the provisional point from all of the complementary information about the registration point  $a_1$  acquirable at the point of completing the assignment of the provisional point and receipts at the registration points  $a_1$  and  $a_2$ , is referred to as a propagation procedure for completion, wherein

5           the incremental completion is carried out without forming a tree structure by the steps of:

          originating in calculating or acquiring all of the complementary information about a registration point  $a$  of the user apparatus, which information is acquirable at a point of completing the assignment of the provisional terminal point, from the certificate that the user apparatus received and stored, the  
10       registration point  $a$  being closest to the provisional terminal point on a left side thereof;

          starting a calculating process of all of the complementary information about respective registration points on the left of the provisional terminal point, which information is acquirable at a point of completing an assignment of the  
15       provisional terminal point, from a rightmost registration point  $a$  of the registration points; and

          applying the calculating process on the registration points on the left of the registration point  $a$  in sequence while using the propagation procedure for  
20       completion.

63.       The program for validation of event-ordering certificates of any one of claims 56 to 62, wherein the incremental completion is accomplished by a method comprising the steps of:

25           extracting respective registration points up to the provisional terminal point appropriately;

          dividing into local areas each between the registration points extracted;

          performing an incremental completion on the assumption that a rightmost assigned registration point in each of the local areas is a provisional terminal point;

30       and



calculating all of acquirable complementary information about the extracted registration points.

64. The program for validation of event-ordering certificates of any one of  
5 claims 56 to 63, wherein

the certification apparatus has electronic information publishing means configured to publish the root value of the sequential aggregation tree electronically after completing the regular time interval; and

the program for validation of event-ordering certificates allows the user  
10 apparatus to perform:

a root-value calculating step of calculating a root value of the sequential aggregation tree from an information about the designated registration point and the complementary information calculated at the incremental completion step after completing the regular time interval; and

15 a root-value validation step of verifying whether the root value published electronically coincides with the root value calculated.

65. An event-time validation program readable by a computer that verifies a time when the user apparatus executing the program for validation of  
20 event-ordering certificates of claim 48 or 52 applies on the event-ordering request, wherein the event-time validation program allows the computer to perform:

an audit result acquiring step of acquiring the audit result;

an event-ordering request acquiring step of acquiring the event-ordering request corresponding to the audit result;

25 a time validation step of judging validity of the third time on a basis of a time difference between the third time and at least either the first time or the second time; and

a step of outputting the judgment.